Social Order in Cyberspace

Xingan Li, LLD
Department of Information Technology, Faculty of Mathematics and Natural Sciences, University of Turku.

Preface

The present work puts social order, security and criminal phenomena on a platform of informed society with the pervasion of information and communications technology. Cyberspace looms in Weberian string of social thinking and shaping an informed rationality out of uninformed rationality, uninformed irrationality and informed irrationality. Regulatory mode for cyberorder can be complex, and ability-and-utility-oriented control should be preferred. Cybersecurity emerges as a critical concept in informed social order, despite its relativity, and optimality through mixed provision. Whenever cybersecurity is not guaranteed, criminal and victim wrestle on an unbalanced stage: the former has always legerdemains to abuse new technologies, while the latter is always vulnerable. Both domestic and international laws are seeking informed solutions to informed threats. Articles in this book can be identified as independent articles, yet they are also to some extent integrated into a systematic structure in nature.

Synopsis

Title: Social Order in Cyberspace

Introduction:

The development of information and communications technology (ICTs) brings about broad survival space for both individual and organizational users. Electronic life becomes usual practice, with indicators such as growth of the number of personal computers and Internet users, the increase in the number of web sites, Internet hosts and web pages, bandwidth growth, the growth of scale of e-commerce and e-governance. People connected through information systems might neither necessarily be as good as within a Weberian formally rational regime, nor necessarily be as bad as in a Hobbesian "war of all against all", nor as ideal as Platonian *Republic*, and Moresian *Utopia*. Cybersecurity can only be perceived as a relative concept. Vulnerabilities of the information society loom, however, on the horizon of people's longing for an optimistic future. Netizens are surprised at the rise of threats of malicious codes to information security of states, enterprises and individuals, for instance. As far as cyberinsecurity and cybercrime are concerned, people have puzzled their brains to find workable solutions. Currently, there is still a necessity for further exploration into the maintenance model suitable to the fresh structure and feature of cyberspace.

Theme/Focus area:

The book will put social order, security and criminal phenomena on a platform of informed society with the pervasion of information and communications technology. Cyberspace looms in Weberian string of social thinking and shaping an informed rationality out of uninformed rationality, uninformed irrationality and informed irrationality. Regulatory mode for cyberorder can be complex, and ability-and-utility-oriented control should be preferred. Cybersecurity emerges as a critical concept in informed social order, despite its relativity, and optimality through mixed provision. Whenever cybersecurity is not guaranteed, criminal and victim wrestle on

an unbalanced stage: the former has always legerdemains to abuse new technologies, while the latter is always vulnerable. Law in East, law in West, and law in globe are seeking informed solutions to informed threats. Articles in this book will deal these issues within a loosely defined framework.

Book Plan:

The book contains articles relating to a new unique discourse on fundamental issues in cyberorder, cybersecurity and cybercrime.

Target Group:

The book is valuable for researchers, scholars, students, lawyers, legislators, and law enforcement officers.

Overview (1500-2000 words)

"Cyberspace and the Informed Rationality of Law" argues that the change of legal system in the environment where the pervasive use of information system forms an irresistible force in shaping nearly all lives of the society needs specific attention. The discussion in this paper briefly defined the limit of its boundary. While we have the very reason to exclude the so-called virtual space from the current field, we make no attempt to negate the value of further inquiry into the all the unique respects brought about by the development and understanding of the new technologies, which in turn indeed leads the old legal thinking up to a novel platform. It is on this higher level that the hypotheses of improved legal literacy and informed rationality operate. The essay's other objectives are to construct the models of order in cyberspace over which internal and external forces exercise control to varying degrees. Although the information society in general and the cyberspace in particular is designed toward an environment accommodating a more ideal legal system, mechanistic calculable justice standard would not be realizable in an optimistic future.

An increasing necessity for building cyber order through legal instruments has existed as one of many alternatives to regulate the world dominated by the globally connected Internet. While cyberspace is global and cyber-activities have remote reach, laws, which are different from one country to another, have been historically designed to deal with acts occurring within territorial limitations. For several years, numerous explorations into possible arrangements, from super-national, international to national laws in separate countries that can possibly be applied to maintain cyber order have been flawed in balancing interests of users and regulators of different jurisdictions. Traditional spatial divide between jurisdictions has been precisely transplanted into cyber-laws. "Exploring into Regulatory Mode for Social Order in Cyberspace" discusses legal gaps of cyber-laws among different localities, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. The official action must be within the ability of the controller so that it can be effective, and that it must also cope with the utility of the controller so that it can be efficient.

In "Legal Roles of Information Systems," information is classified according to its value into five categories, including information with positive value, value-neutral information, valueless information, information with negative value, and information that its value is disputable. The article further analyzes the interaction between information and criminal law, particularly the necessity for criminal law reform in the information age.

Based on the relative concept of cybersecurity, "Mixed Provision of Cybersecurity" analyses the economic impact of cybersecurity breaches, identifies cybersecurity as a private good, and claims to implement the approach of mixed provision. The security protection should be principally borne by the private sectors, but the government is able to play an important role in establishing and enforcing the liability mechanisms. The mixed provision indicates that the close cooperation between the public and private sectors in security protection.

While the growing scale of Internet use brings about great convenient for users, phenomena of unsolicited e-mail pose new threats and challenges. Previous literature was concentrated on general analysis of such messages, leaving many particular respects untouched. This study focuses on the extension of victimization of unsolicited messages e-mail with attachments (UEMAs). Based on the analysis of two samples, one comprised of 501 (sampling done in May 2006), and the other comprised of 490 (sampling done in March 2008),pieces of UEMAs, "Extension of Victimization: Unsolicited E-mail Messages with Attachments" finds that e-mail account exposing and seeking can both contribute to victimization; while receiving of unsolicited messages is the initial victimization, reading and reacting to messages could lead to additional victimization from virus attack or financial fraud, and from conspiracy in illegitimate operations such as tax evasion or transaction of falsified documents.

Fight against cybercrime necessitates better knowledge about the characteristics of cybercrime. "Critical Factors in Combating Cybercrime" is designed to make a synchronic inquiry into the characteristics of cybercrime in comparison with traditional offences. The article identifies a number of factors that complicate the reporting, detection, investigation, prosecution, conviction, and sentencing of cybercrime. The themes explored in this paper show that there is no easy way of bringing cybercriminals before the judicial process. Nevertheless, the increase of cybercrime is constant, and the reinforcement of deterrence is a constant need, yet for

these two forces to reach equilibrium is still an on-going process.

"Domestic Platform for Social Order in Cyberspace: the Case of China" provides a study on the criminalisation of cybercrime and control over the Internet in China. In order to exercise control over the Internet, China took a series of actions characterized by criminalization of cybercrime, content filtering and activity monitoring, in order to maintain the state stability as well as cybersecurity. The recruitment of cyber police, the investment on security technology, the requirements on the Internet enterprises, and the surveillance on the users, form a close net to prevent cybercrime.

"International Platform for Tackling Cybercrime" reviews the international impetus of criminal law reform in combating cybercrime. This article classifies actions of international harmonization into professional, regional, multinational and global actions, summarizes the major concerns of these actions, and concludes the influence of the Convention on Cybercrime on state and international levels of legal countermeasure. The article also points out the limitations of the previous actions and anticipates the United Nations to play a more important role.

Snapshot (220-270 words)

The development of information and communications technology brings about broad survival space for both individual and organizational users. Electronic life becomes usual practice. People connected through information systems might neither necessarily be as good as within a Weberian formally rational regime, nor necessarily be as bad as in a Hobbesian “war of all against all”, nor as ideal as Platonian *Republic*, and Moresian *Utopia*. Cybersecurity can only be perceived as a relative concept. Vulnerabilities of the information society loom, however, on the horizon of people's longing for an optimistic future. Netizens are surprised at the rise of threats of malicious codes to information security of states, enterprises and individuals, for instance. As far as cyberorder is concerned, people have puzzled their brains to find workable solutions. Currently, there is still a necessity for further exploration into the maintenance model suitable to the fresh structure and feature of cyberspace.

The book puts social order on a platform of informed society with the pervasion of information and communications technology. Cyberspace looms in Weberian string of social thinking and shapes an informed rationality out of uninformed rationality, uninformed irrationality and informed irrationality. Regulatory mode for cyberorder can be complex, and ability-and-utility-oriented control should be preferred. Cybersecurity emerges as a critical concept in informed social order, despite its relativity, and optimality through mixed provision. Whenever cybersecurity is not guaranteed, criminal and victim wrestle on an unbalanced stage: the former has always legerdemains to abuse new technologies, while the latter is always vulnerable. Globally, law is seeking informed solutions to informed threats. Articles in this book will deal these issues within a loosely defined framework.

Snapshot (150 words)

People connected through information systems might neither necessarily be as good as within a Weberian formally rational regime, nor necessarily be as bad as in a Hobbesian "war of all against all", nor as ideal as Platonian *Republic*, and Moresian *Utopia*. The book puts social order on a platform of informed society with the pervasion of ICT. Cyberspace looms in Weberian string of social thinking and shapes an informed rationality out of uninformed rationality, uninformed irrationality and informed irrationality. Regulatory mode for cyberorder can be complex, and ability-and-utility-oriented control should be preferred. Cybersecurity emerges as a critical concept in informed social order, despite its relativity, and optimality through mixed provision. Whenever cybersecurity is not guaranteed, criminal and victim wrestle on an unbalanced stage: the former has always legerdemains to abuse new technologies, while the latter is always vulnerable. Globally, law is seeking informed solutions to informed threats.

Acknowledgements

Without the inspiration, facilitation, and help of different institutions, persons, and platforms, this book will simply remain impossible. This book comes directly from my postdoctoral research. I thank Faculty of Law, University of Turku for permitting me to pursue postdoctoral research. I am particularly grateful with Professor Dr. Ahti Laitinen, supervisor of my doctoral study, Professor Dr. Heikki Kulla, Dean of the Faculty, and Ms. LL.M. Milla Erkola, Head of Administrative Affairs of the Faculty, and other academic and administrative personnel at the faculty, who make my research procedurally and substantively possible.

I thank Ms. Asifa Begum, Consulting Editor at Amicus Law Books Division, ICFAI University, India, for her interest in reprinting my published articles and soliciting my new articles on various issues revolving cyberlaw. It can be said that it is her interest and encouragement make my research and writing progress faster than ever. It is also Ms. Asifa Begun's proposal makes this book such framed. I want to also to thank the review committee for their comments and suggestions on the title and content of this book. In fact, I accepted their suggestion on the title of this book.

When I published my doctoral dissertation, our family were waiting for the birth of our fourth member. I left our family unacknowledged in that book. Today, I have to, and am pleased to give appreciation to our four-member family with full credits for their longstanding support for, tolerance with and understanding of my monotonous, simple and austere research life. Thank you, Shuiqing, Dinah Peilin, and Tarja Peiyun. I would also like to express my gratitude to my parents, brothers and sisters for their longstanding spiritual support.

Turku, 1 March, 2009 Xingan Li

Copyright lines

Chapter I Cyberspace and the Informed Rationality of Law, was originally published in Ahti Laitinen ed. Writings *in the Sociology of Law and Criminology*, University of Turku Faculty of Law, 2006. Reprint with permission.

Chapter II, new writing.

Chapter III, Legal Roles of Information Systems, was originally published in "*Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*", University of Turku, 2008, Turku: Uniprint. Reprint with permission.

Chapter IV, new writing.

Chapter V, new writing.

Chapter VI Critical Factors in Combating Cybercrime, was originally published in my "*Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*", University of Turku, 2008, Turku: Uniprint. Reprint with permission.

Chapter VII, new writing.

Chapter VIII International Platform for Tackling Cybercrime, has been developed from "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene," originally published in *Webology*, 4(3), 2007. Available at: http://www.webology.ir/2007/v4n3/a45.html. Reprint with permission.

Photograph



Photo by Peilin Li (1 March, 2009)

Big Profile (100-120 words)

Xingan Li, LLB (Inner Mongolia University 1989), LLM (China University of Political Science and Law 1994), LLD (University of Turku 2008), is doing postdoctoral research at Faculty of Law, and is a researcher at Department of Information Technology, Faculty of Mathematics and Natural Sciences, both of University of Turku. He lectured on Cybercriminology at Turku Law School in spring 2009. He lectured on criminal law, criminology, criminal psychology, and procedural law at Inner Mongolia University, China (1995-2003). He was a visiting scholar at Kyushu University, Japan (2000-2001). His research interests range from criminal law of China, England and Japan, criminology (particularly, cybercriminology), criminal psychology, procedural law, human rights, modern Japanese religion, to application of information systems to crime research. He published more than 50 articles and more than ten books in Chinese and English.

Small Profile (50 words)

Xingan Li, LLB (1989), LLM (1994), LLD (2008), is doing postdoctoral research at Faculty of Law, and is a researcher at Department of IT, both of University of Turku. He taught criminal law, criminology, criminal psychology, and procedural law at Inner Mongolia University, China (1994-2003). He was a visiting scholar at Kyushu University, Japan (2000-2001). His recent research interests are cybercrime and work informatics.

Index

Hacker

Hacking

Human-machine interaction step (HMIS)

Information age

Information and communications technology (ICT)

Information society

Information systems

Informed rationality

International cooperation

International harmonization

International platform

Internet

Interpol

Japan

Jurisdiction

Law

Machine-human interaction step (MHIS)

Machine-machine interaction step (MMIS)

Malicious code

Mixed provision

Network

Nordic countries

OAS

OECD

Penal law

Private good

Regulation

Regulatory mode

Relativity

REMJA

Social order

Spyware

Terrorism

U. S., the

UEMA

UN

Unauthorized use

Unsolicited e-mail message (UCE)

Victimization

Virtual space

Worm

Table of Contents

Index of Figures

Index of Tables

Chapter I Cyberspace and the Informed Rationality of Law

Abstract

The change of legal system in the environment where the pervasive use of information system forms an irresistible force in shaping nearly all lives of the society needs specific attention. The discussion in this paper briefly defined the limit of its boundary. While we have the very reason to exclude the so-called virtual space from the current field, we make no attempt to negate the value of further inquiry into the all the unique respects brought about by the development and understanding of the new technologies, which in turn indeed leads the old legal thinking up to a novel platform. It is on this higher level that the hypotheses of improved legal literacy and informed rationality operate. The essay's other objectives are to construct the models of order in cyberspace over which internal and external forces exercise control to varying degrees. Although the information society in general and the cyberspace in particular is designed toward an environment accommodating a more ideal legal system, mechanistic calculable justice standard would not be realizable in an optimistic future.

Keywords: cyberspace, informed rationality, law

Introduction

Inventions and innovations during the last two or three centuries have extraordinarily revolutionized the landscape of human society that has a recorded history of several millennium. Change, which could take a variety of styles, is not inevitably equivalent to advancement and improvement. Consequently, both constructive changes and unconstructive changes, both active changes and passive changes have been taking place where there are appropriate conditions and contexts. Introduction of and pervasive dependence on computer information systems since the 1940s is one of such changes that utterly improves the general excellence of social life on one hand, and inexorably worsens certain aspects on the other. Contemporary society steps into an inconvertible position of deep addiction to this artificial instrument: while the efficiency of production has been constantly enhanced, the foundation of conventional social control is challenged and shaken.

Information systems could hardly be cerebrated as of beneficiality or harmfulness according to an amalgamated criterion. Even such a criterion is unavailable due to the diversity of people's attitudes towards the value of overflowing information. The general public, nonetheless, have always been predisposed to standing in a position to pose it as a positive factor that assists interpersonal and international communication. The common use of "information systems" and various other relevant terminologies, as a result, is in a sense not neutral, but is value-laden. It is as good as spiritual and material assets. Some others also recognise the difficult issues in identifying the real value behind the surface of the illusory common knowledge about this new technological and social phenomenon: people connected through information systems might neither necessarily be as good as within a formally rational regime as Max Weber stated, nor necessarily be as bad as in "bellum omnium contra omnes" (La. the war of all against all) as Hobbes' *Leviathan*,[1] nor as ideal as Plato's *Republic*, and Thomas More's *Utopia*. All the possible views are, however, in existence in defining the sphere of legal status of cyberspace.

This article will be devoted to identify the change, if not all improvement, of legal systems in the environment of information systems. In the next section, the article will first define the sphere of this discussion to exclude the so-called virtual space from cyberspace, pointing out that the virtual space in the psychological and imaginary sense is not relevant in addressing law. The article will be subsequently concentrated on the issues of legal literacy. Information systems improve the enhancement of legal literacy on one hand; it posits the focus on informed rationality on the other. Formal rationality is one of the four ideal forms of law and legal thought constructed through Weber's two-dimensional coordinate system including "formality" and "rationality" (See Milovanovic 1994, pp. 40-47). The article depicts the revised model of Weber's ideal form of law and legal thought, putting Weber in a three-dimensional coordinate system. The article also considers the relationship between internal and

[1] The Latin phrase itself was first presented in the preface of De Cive (La. The Citizen): "Ostendo primo conditionem hominum extra societatem civilem (quam conditionem appellare liceat statum naturae) aliam non esse quam bellum omnium contra omnes; atque in eo bello jus esse omnibus in omnia." (Hobbes 1839, p. 148. La. I demonstrate in the first place, that the state of men without civill society (which state we may properly call the state of nature) is nothing else but a meere warre of all against all; and in that warre all men have equall right unto all things. The English translation is cited from a version printed by J.C. for R. Royston, at the Angel in Ivie-Lane, 1651, available online at http://www.constitution.org/th/decive00.htm.)

external control over the cyberspace order. Finally, the article discusses the infeasibility of the idea of computerized justice system.

Exclusion of conceptual virtual space

During the 1990s, there emerged many comments conceptualizing cyberspace as an unadulterated and uncontaminated "virtual space" (Mason 1998), having no involvement of people, society and state. Neither would cyberspace invade and infringe society, nor would society invade and infringe cyberspace. Under such a perspective, cyberspace could be explained as a space mirage existing in information-systems-facilitated games, communications and germane economic transactions. The most noteworthy instances were where "virtual rape" was perceived by a number of authors to be committed (Dibbell 1993) and losses of virtual property were undergone (The concept of virtual property have been be defined in various ways particularly in articles by different authors of different disciplines, for a few examples, see Bartle 2004; Fairfield 2005) by cyber game role-players. Under such circumstances, I understand that a virtual space is an imaginary space (not necessarily a place) where real human individuals exist and behave behind a curtain of sign, symbol, or graphic-being represented by bits and bytes of digits. Virtual rape is not human physical experience but rape during which a feminine sign, symbol, or graphic-being manoeuvred by a human player (not necessarily a female) is subject to a position of similar psychological and imaginary suffering through activities by a masculine sign, symbol, or graphic-being manoeuvred by another human player (not necessarily a male). Thus far virtual rape is not rape in legal sense, even to the dawn of the information age.

A virtual property is a sign, symbol, or a graphic-being available with the cost of real money, that is, it has use value and exchange value and is a commodity, even though it exists only within the sphere of information systems.

While we are barely convinced to accept a case where virtual rape is comparable to real rape and subject it to the criminal justice system, we are prone to confirm the status of virtual property as real property, because it has the same attributes as that of a real property: exchangeability through the intermediary of money.

Once "virtual property" enters the sphere of circulation through the intermediary of money, be it a sign, a symbol, or a graphic-being, it becomes a thing that we are measuring through such a ruler as value. It does no longer stand still in the pure

psychological and imaginary sphere as ambiguous as virtual rape. It comes out of virtual space and goes into real life. If we own this "virtual" property valued one million dollars, we are millionaires through the value of this sign, symbol, or the graphic-being. If burglars or robbers take this "virtual property" away from us, we are suffering from a big bite out of our cakes. It is now no longer "virtual" at all.

When we explore law in cyberspace, we are not discussing about anything that is so unperceivable as virtual rape, or virtual space. Rather, cyberspace is simply an extension of real space, meat space, or our society, the extension of this society through the facilitation of information systems that connect many in different temporal and spatial distributions into globally accessible, 24/7/365 available, and linguistically-interpretation-powerful networks. Society has been a web, but this is a social web of new style with intervening factors of machine filling situated in the human-human interaction process. The new social web is constructed more by instant and remote chains of human-machine-human interactions. The quantity of face-to-face human-human interactions is seen decreased and its role weakened.

The social order along the newly-emerged social ties, however, would not be expected to turn over the fundamental social order. Rather, the conventional social order would be to operate continuously with the assistance of machine-enabled mechanisms. People, societies and states should not enter a cave or hole as virtual as a psychological and imaginary space and begin their exploration into the value of existence from the beginning. Law and order would become more realistic and simplified if our conventional mechanisms run in an operable way as in the past. Cyberspace thus gives more sense to the extent that its existence empowers the existing social order, regardless of it being reasonable or unreasonable. In sum, the creation of cyberspace extends the sphere of existing society, but not carries the function of undermining the current society or separating itself from the traditional one.

Improvement of legal literacy

Although cyberspace would not be as bizarre as a society that is as virtual as a psychological and imaginary phenomenon, it would bring about changes for the present status of society. Cyberspace is a new field and a new frontier that runs law and order of our society as a programme. It does more than merely copying, duplicating or repeating conventional modes of forms of law and legal thought.

Quality of the legal framework and effect of its operation are severely dependent on legal literacy of citizens. Traditionally, legal illiteracy is not even a reason for citizens to be more or less excused, because there is such legal maxim as "ignorantia juris non excusat" (No-one should be excused for ignorance of the law). Here, by legal literacy, we refer to the condition of knowing law by people subjecting them to the order under the constraint of law.

As far as legal literacy is concerned, the degrees to which literacy exists differ from one to another. There are those who are rather legally illiterate, who are more or less legally literate, and those who are highly legally literate. Certainly, there is hardly one who is absolutely legally illiterate and one who is completely legally literate. Literacy exists on one certain point along the line of degrees between zero percent and one hundred percent. Thus far, we can list ideal types of citizens according to different degrees of their legal literacy:

1. Those who are illiterate are also legally illiterate of both domestic law and foreign law.

2. Those who are literate but are legally illiterate of both domestic law and foreign law.

3. Those who are literate are also legally literate of domestic law but not foreign law.

4. Those who are literate are also legally literate of foreign law but not domestic law.

5. Those who are literate are also legally literate of both domestic law and foreign law.

The reasons why citizens are illiterate of law are multiple, but two of them are of the most significance: the unawareness of citizens and the unavailability of law.

The unawareness of law was once a primary factor for citizens to hold an alienate attitude towards any law, be it of civil or criminal nature. In many countries in previous centuries, ties with something "a law" were somewhat bad, unfortunate or mystery. Therefore, persons who were assigned as subjects operating law would be mystified as a result of their priority over power and knowledge, through such symbolic things as crosiers and ritualistic robes; persons who were involved in legal issues would be categorized as either vulnerable individuals who suffered from infringement or invasion from others, or vulgar individuals who imposed infringement or invasion on others. As a whole, law is not a usual practise in daily

life and social activities. On the contrary, escaping from law and relevant affairs was preferred by a majority of citizens.

The awareness of law has been increasingly strengthened over years due to the seriousness and severity of legal issues being decreased and the position of the legal profession being demystified. The current situation is that even though no one knows everything about law, most citizens know something about law. The legal profession is gradually becoming a profession that is increasingly comparable with other specialities, in Durkheim's words, different divisions of labour, in society. Therefore, unawareness of law is gradually becoming a minor reason why citizens are legally illiterate.

The other important reason why citizens are legally illiterate is the unavailability of law. In ancient times, the universal practise was that "if the penalty remains unknown to all, its power would be immeasurable." (The words are from the comments by Kong Yingda, a Chinese writer in Tang Dynasty on a classic *Zuozhuan* in the volume of Zhaogong) The function of earlier law was supposedly repressive (See Durkheim 1933). For the ruling class to maintain the repressive ruling order, grasp, control, monopoly, and manoeuvre of the mysteriousness of the legal power is of necessity. With the change of the legal function, the "keeping-unknown" of law became not so important in maintaining the mysterious power of the state. Thus this issue became less significant in unavailability of law. The notion was only one side of the coin of the unavailability of law that kept law far from the reach of citizens. The other side of the coin was that conditions of transportation and communications in the ancient times made it impossible to inform most population of law.

Thus, the active refusal of law on one hand, and passive refusal of law on the other, severely impeded the widespread of legal bodies, legal knowledge and legal consciousness. The coming of the legal enlightenment did not happen until the end of the Middle Ages. Thomas Paine stated the principle of rule of law in 1776: "For as in absolute governments the king is law, so in free countries the law ought to be king; and there ought to be no other." (Paine 1844, p. 28)

In modern times, it is not the actual fact that citizens are legally well informed. Even today, states are not fully making efforts to inform their citizens of law. But there is an interfering element in spreading law: the invention of electronic digital computer and the connection of information systems through the publicly-accessible networks. Once the printing technique and wide-distributed libraries made it possible

that every citizen could access to available bodies of law. However, it is not a situation where law is available without the limit of time and space. Contemporary information systems change the picture of legal availability and accessibility in providing the possibility of superseding the spatial-temporal boundary of looking up a printed copy.

Other facilities and inventions did ever improve the availability of law, such as postal system, telephone, telegraphy, and facsimile. But the severe dependence on human resources and the high expenses still left it unreachable to most of the population. Current information systems seemingly apparently overcome the shortcomings of traditional media.

However, we must bear in mind that doing law (doing medicine, and doing many other scientific practices) is not like doing dictionary looking-up. What we view, read and understand does not equal to what we would receive the reading from specialised legal agencies. Therefore, specialised legal agencies are not substitutable through the common reading of law and widespread of legal knowledge. But it is to satisfy citizens to have a better chance to access to existing law, legal knowledge and achieve higher legal consciousness. All this will help to demystify the legal bodies and the legal profession, and to maintain legal rights and limit the arbitrary power.

Informed rationality

When Weber proposed his ideal models of form of law in *Economy and Society*, he had hardly the concern about whether citizens were legally informed or not. Therefore, we could imagine Weber as depicting his models on the premise of citizens being either completely legally informed or completely legally uninformed. But today, we are confronted with increasingly deep concern about the issue whether citizens are legally literate or informed, because we are in an age of being better informable with these tremendous information systems, as we are migratable with the powerful transportation mechanisms.

If we could suppose the ideal model of form of law in the past was uninformed formal or substantive rationality or irrationality, then our model thereafter should be revised as informed formal (or substantive) rationality (or irrationality). Thus we could put Weber's ideal models into a 3-Dimensional coordinate system. Borrowing from Weber's four ideal forms of law and legal thought, plus our extra dimension of informability, then we have (The description part of each item mainly refers to the

induction of Milovanovic 1994. The part of about informability is my own):

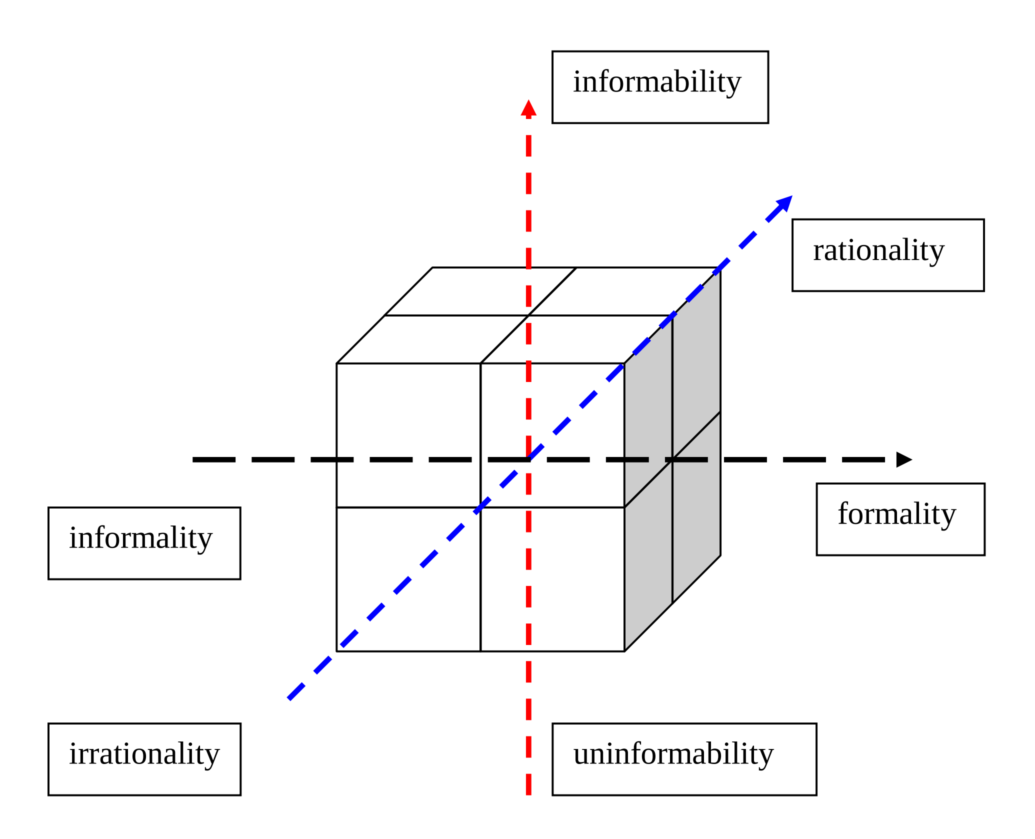


Figure 1 Three-Dimensional coordinate system of forms of law and legal thought

Informed formal rationality. That is formal rationality with the subjects informed. Under this model, the legal system was operated under the circumstances where clearly-addressed and clearly-observed rules were applied to all like cases in a consistent form. Similarly situated were similarly treated, without external interference with the decision-making process. Besides, the decision-making process has higher degree of transparency by ensuring that the subjects are informed of the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and transparent operation.

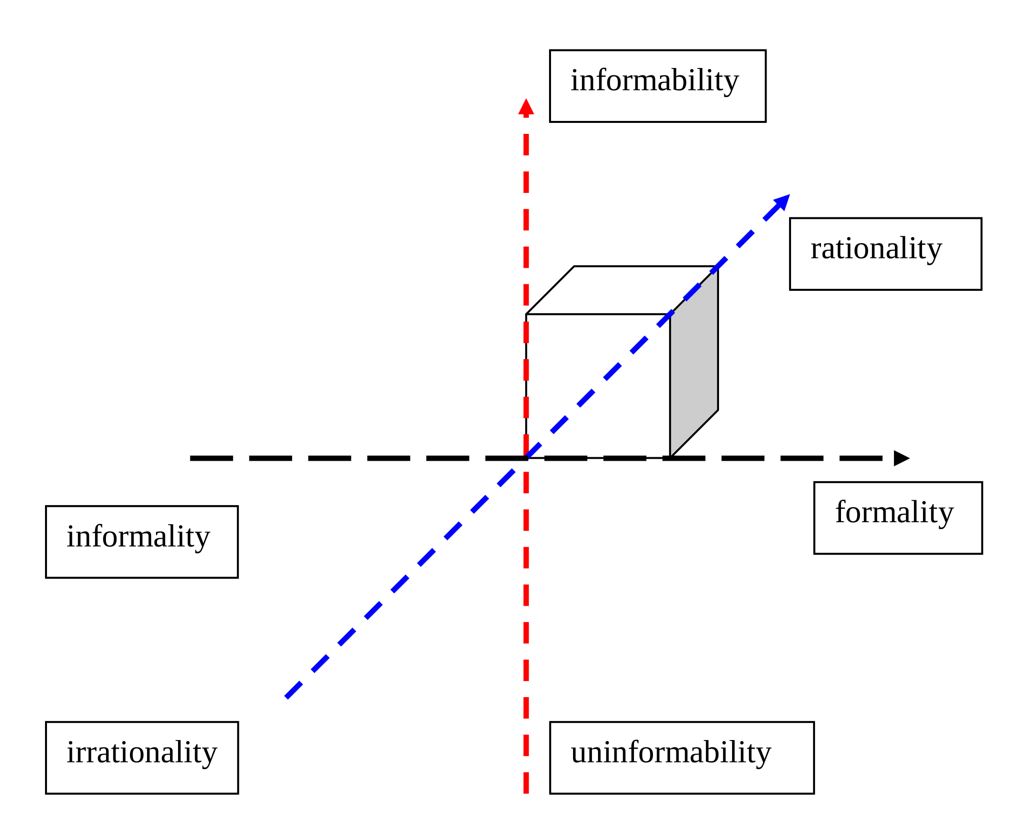


Figure 2 Informed Formal Rationality

Uninformed formal rationality. That is formal rationality without the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were similarly treated, without external interference with the decision-making process. However, the decision-making process has lower degree of transparency and the subjects are not ensured informed of the applicable rules and/or processes. In sum, this model could be trichotomized as unified criterion, due process, and opaque operation.

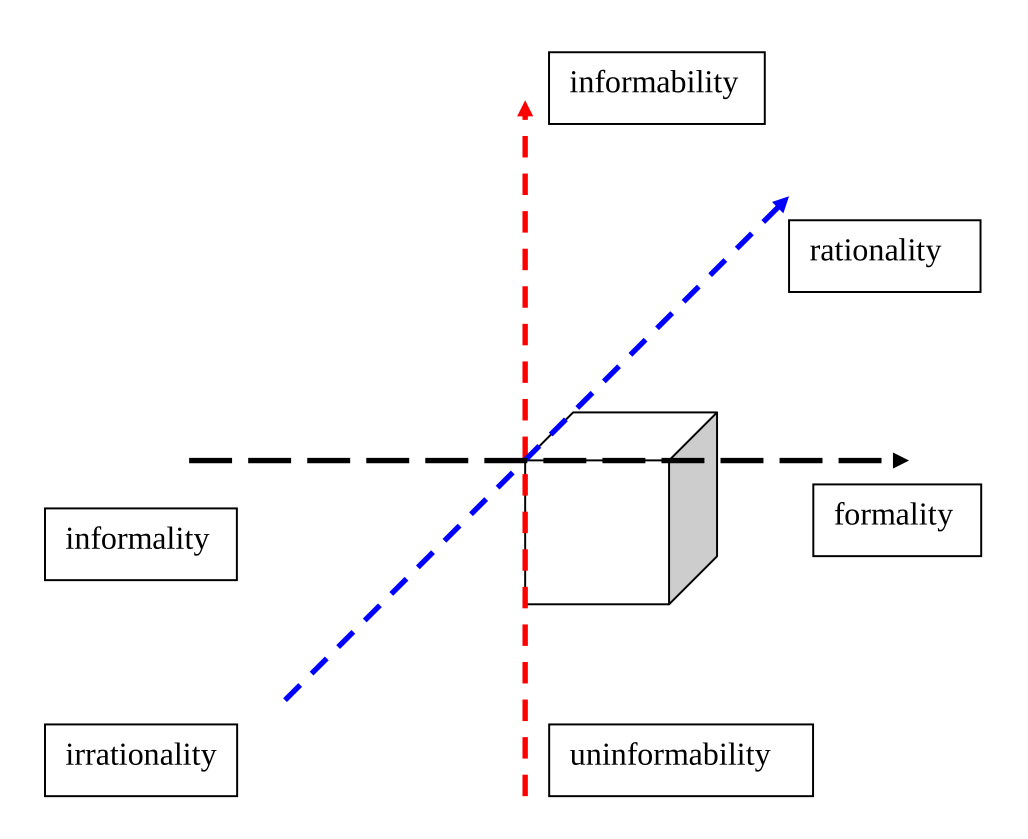


Figure 3 Uninformed Formal Rationality

Informed formal irrationality. That is formal irrationality with the subjects informed. Under this model, the legal system was operated in the process when it is uncertain whether clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were differently treated, with some mysteriously arranged mechanisms functioning in the decision-making process. Arguably, the decision-making process has a certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, due process, and transparent operation.

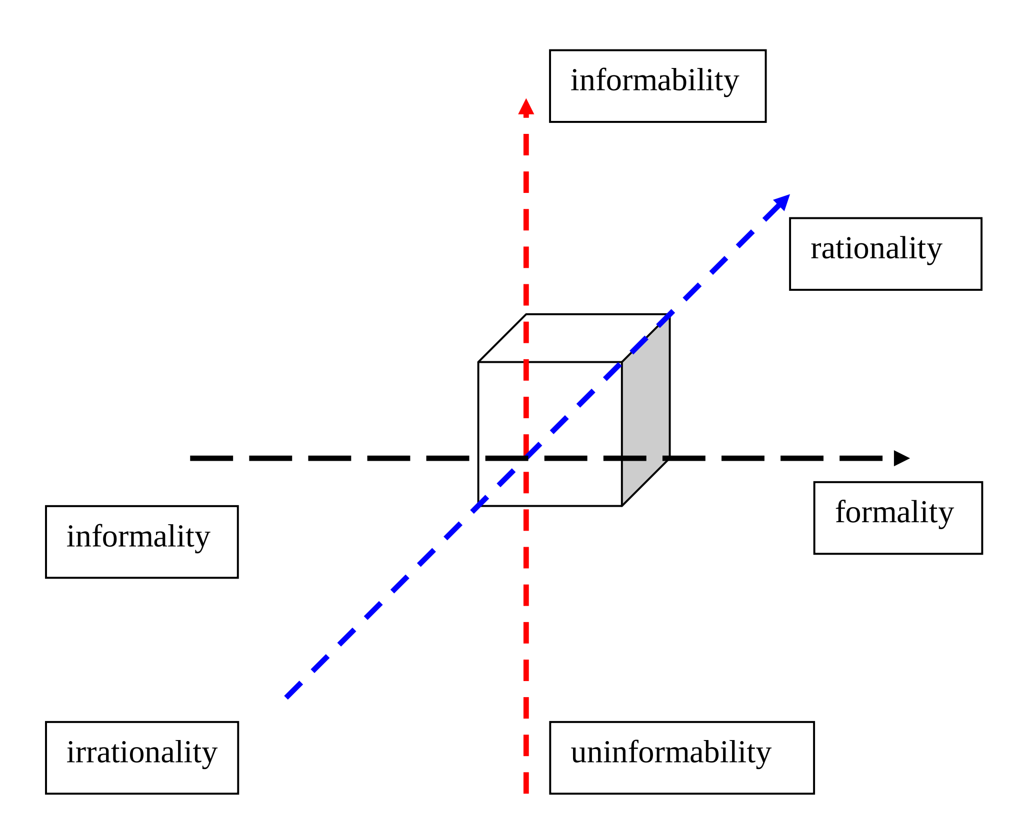


Figure 4 Informed Formal Irrationality

Uninformed formal irrationality. That is formal irrationality without the subjects informed. Under this model, the legal system was operated in the process when it is uncertain whether clearly addressed and observed rules were applied to all like cases in a consistent form. Similarly situated were differently treated, with some mysteriously arranged mechanisms functioning in the decision-making process. The decision-making process was absolutely secret through depriving any degree of transparency by denying opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, due process, and opaque operation.

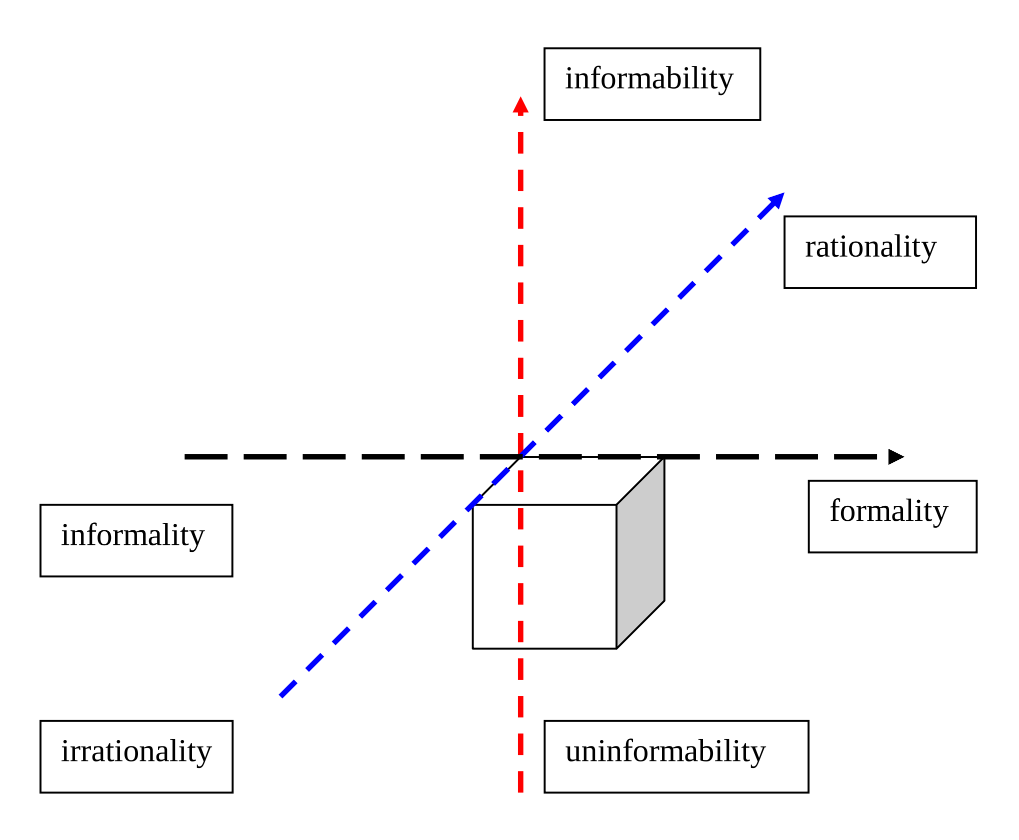


Figure 5 Uninformed Formal Irrationality

Informed substantive rationality. That is substantive rationality with the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to cases according to the detailed situation. Similarly situated were differently treated, with severe external interference with the decision-making process. Besides, the decision-making process has certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and transparent operation.

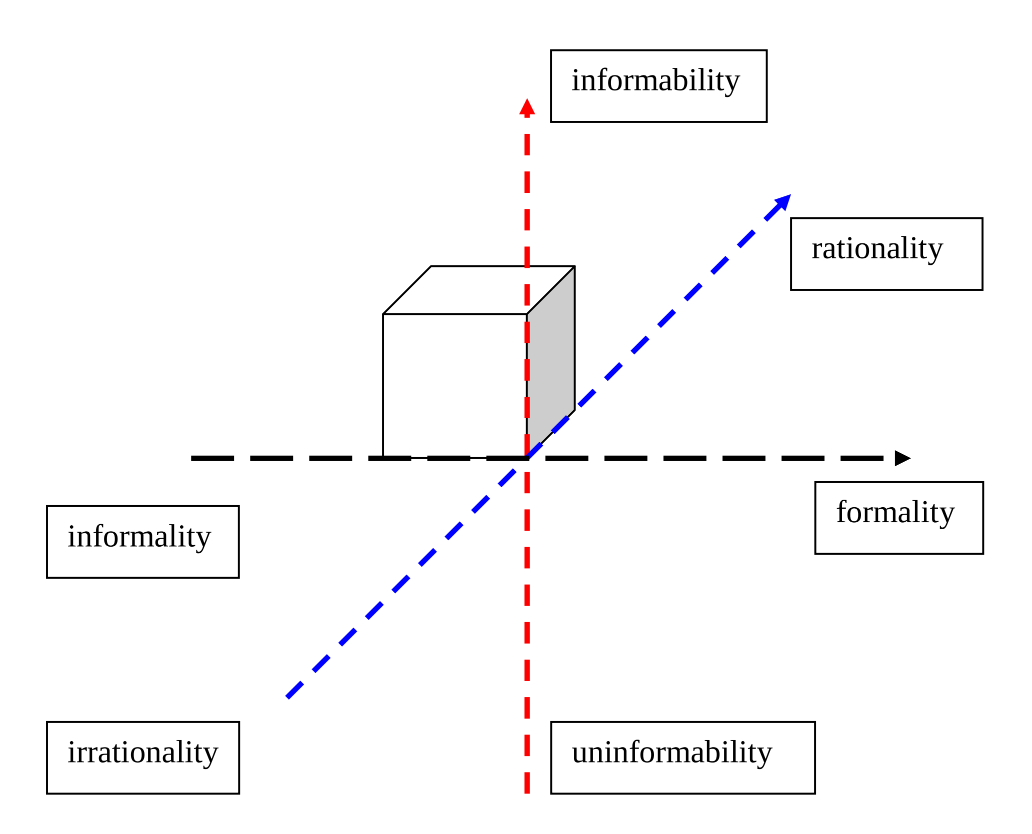


Figure 6 Informed Substantive Rationality

Uninformed substantive rationality. That is substantive rationality without the subjects informed. Under this model, the legal system was operated under the circumstances where clearly addressed and observed rules were applied to cases according to the detailed situation. Similarly situated were differently treated, with severe external interference with the decision-making process. Furthermore, the decision-making process has no transparency due to denying opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and opaque operation.

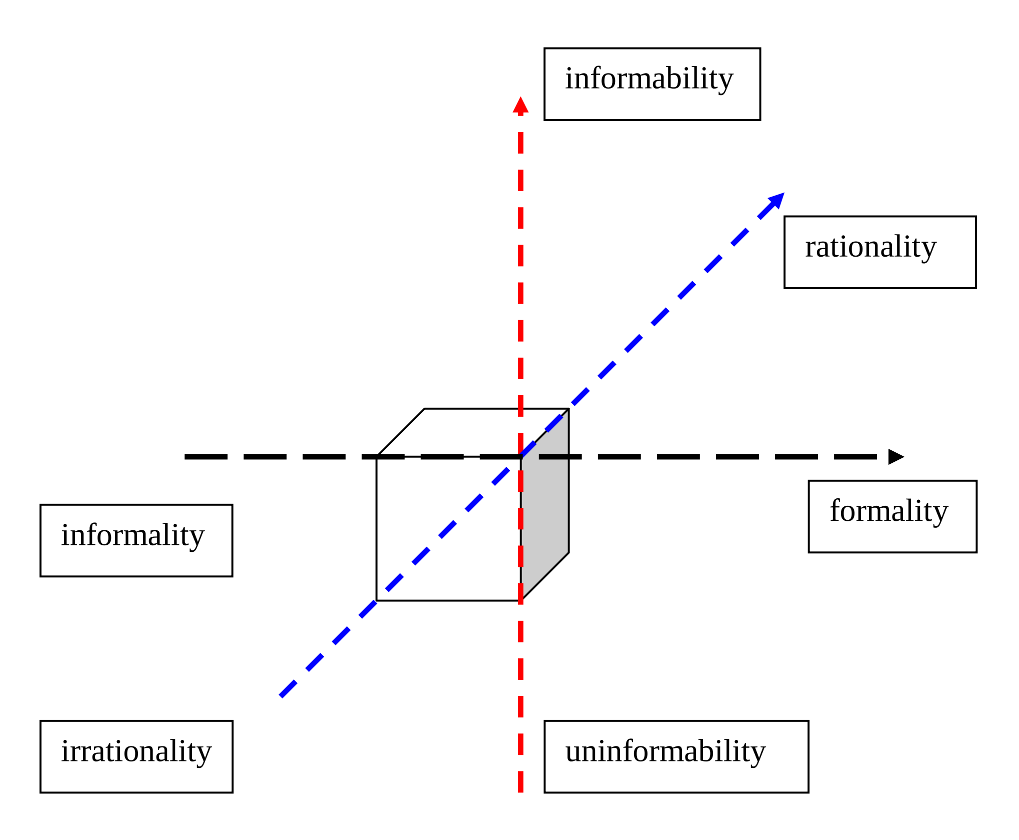


Figure 7 Uninformed Substantive Rationality

Informed substantive irrationality. That is substantive irrationality with the subjects informed. Under this model, the legal system was operated in the process when detailed situation determined the decision. Similarly situated were differently treated, with severe external interference with the decision-making process. Ironically, the decision-making process has certain degree of transparency by providing opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and transparent operation.

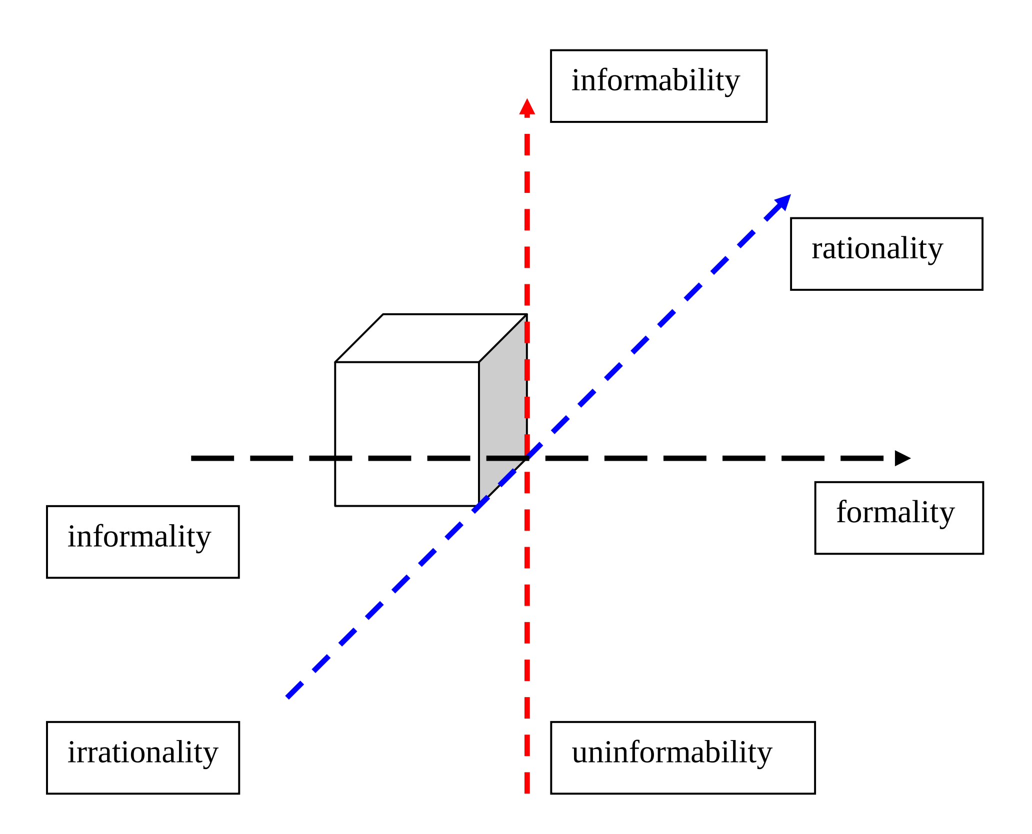


Figure 8 Informed Substantive Irrationality

Uninformed substantive irrationality. That is substantive irrationality without the subjects informed. Under this model, the legal system was operated in the process when detailed situation determined the decision. Similarly situated were differently treated, with severe external interference with the decision-making process. Furthermore, the decision-making process has no transparency due to denying opportunities for the subjects to be informed of the applicable rules and/or processes. In sum, this model could be trichotomized as diversified criterion, random process, and opaque operation.

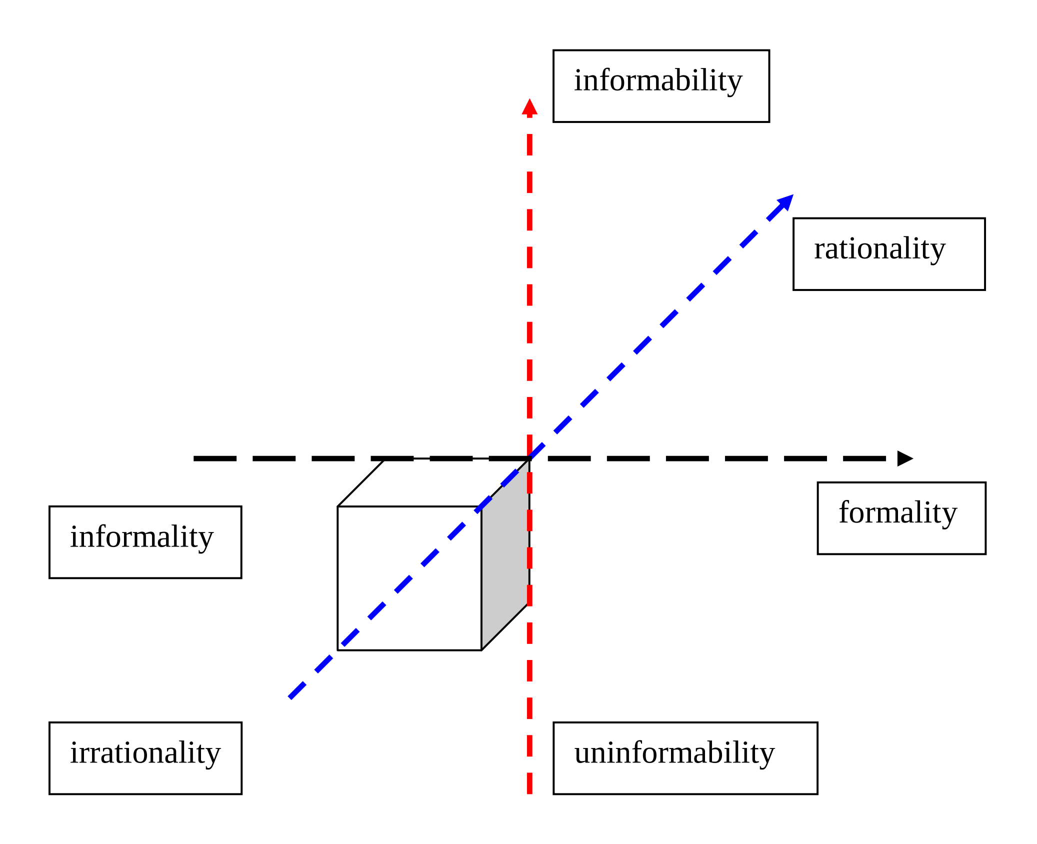


Figure 9 Uninformed Substantive Irrationality

In the past, legal form of law was sunk under the platform of the surface between the informed and the uninformed. That is to say, it was located in a certain point within the part constituted by the points of Uninformability-Informality-Irrationality-Formality-Rationality. Today, it is raised to the level of being informed. Thus we are talking primarily about the informed form of formal (or informal) rationality (or irrationality), located within the part constituted by the points of Informability-Informality-Irrationality-Formality-Rationality. That is the upper part of the coordinate system, which is floating above the surface by information systems.

Limited challenge to the conventional status of legal profession monopoly

In the past, legal profession happened to be highly monopolistic, mainly through control of the texts of law: everyone who wanted to know law is denied the chance to know, except that the legal agencies publicized through some limited fixed form, for example, ancient Roman's The Twelve Tables. The legal system was manoeuvred by a group of people not necessarily the representatives of citizens and operated secretly and mysteriously.

The legal profession was increasingly less monopolistic due to the evolution of

society in general and the more transparency of the legal system in particular. But without citizens being well informed of law, it remained highly secret, mystery and monopolistic: everyone who wanted to know law is neither denied nor granted the chance, but unable to know more.

That the law appears in its real face has never been fully ensured in the history unit now. But with citizens highly informed, the monopoly of legal profession is confronted with strong challenge: everyone who wants to know law is not denied but granted the chance, and able to know. The going-online of the laws and governance into information systems and development of legal retrieval system serves both legal professionals and citizen laymen of access to law. The monopoly of legal profession through control of legal texts becomes uneasy.

The development, however, does not represent a process of breaking up the monopoly of the legal profession in a foreseeable future. Rather, the monopoly is more through control of employment quota and qualification but less through control of bodies of law. This is related to a more important and more complicated issue in which the achievement of the qualification for legal profession could only be possible through the specialised legal training during which only a limited number of people could be taught the legal discourse, which others could hardly grasp through merely reading the clauses of law. Anyway, information systems do not provide systematic law school education. Even it does, it is still different from that the officially qualified legal professionals received in original form of law school. The legal profession thus is determined to be monopolistic, despite that the monopoly of legal texts is less strong than before when there is not a legal retrieval system. In a word, the resistance of the conventional sets of factors of the legal system is not sensitive and vulnerable to the upcoming new challenge.

Primitive Cyber Society

Another dimension we are concerned with is related to the legal order in cyberspace. We could find little evidence on whether the cyber society will repeat or replicate the developmental process of the traditional or non-cyber-society. But we have witnessed a lot of statements that impressed us as if they described the state of the emerging societal existence in relation with information systems as in a primitive stage as that has been had much to be said by writers only in the last several centuries. While whether what they have actually experienced or investigated were

“primitive” societies is still to be determined, we could find a publicly recognized model of primitive society characterized by lower developed culture, economy and political structure. The similar happened in the inquiry of the cyber society and an impression of primitive cyber society is quite clear in current literature.

Hobbes’ Leviathan, and Rousseau’s state of nature were relatively pessimistic scenarios. Marxian primitive communist society was far more an optimistic picture than theirs. In this primitive communist society, there was no private property, no class and class struggle, no state, no deprivation. People commonly owned productive materials and living materials, commonly worked and lived, and equally distributed products. Only when private property, the source of all evils, emerged did the primitive society become involved into conflicts of interests. Despite all these distinction between the viewpoints on how the primitive society existed, the twentieth century observers from different standpoints viewed the emerging cyber society as different as those who observed the primitive societies several centuries ago.

Classic writers wrote on the primitive societies from relatively post de facto positions, while the modern writer writes the primitive cyber society from relatively priori de facto positions. It could be safely said that the classical writers hardly ever lived a practical life in the primitive societies they investigated, heard, wrote or imagined. At best they were outside observers of some of the objects, which there were not enough convincing evidences to prove us that they were the just models that preceded societies of our, or more exactly, of the classical writers, they were inquiring. In fact, the practical primitive societies of the current mainstream societies remain unknown to present people. Cyber society, however, has been closely witnessed by many of the commentators who are writing about the developmental process of it. Therefore, the primitive cyber society might be one of the primitive societies that has ever been mostly investigated and written, if there was ever another one that was investigated and written by writers in person.

Internal and external control of cyber society

Control over a society can be mobilised by either internal or external factors, or in case there is no control at all, by neither internal nor external factors. But it is a rare case where there is no control, or no order at all. However, most writers are claiming that the cyber society is not regulation-free, because order exists everywhere maintained by certain internal or external control mechanisms.

Society could be regarded as integrity, of which cyberspace is a part. The order of cyberspace is also a part of the integrative order of society. Cyberspace as a social existence, however, has special patterns and could be defined as a sub-societal unit. The order maintenance in cyberspace, therefore, could be achieved by internal control and/or external control (for society as a whole, it is still internal control).

Those who wrote a little about the organizational forms of cyber society only wrote about what they observed and found. In order to understand the full picture of the complicated situation of the possible organizational forms of a society, we should use the ideal models of the internal and external control to simplify observations and descriptions of it.

An order can be maintained by either internal or external mechanisms in different degrees. The internal control is the order maintenance through the internal mechanisms within the cyberspace. That is to say, the netizens self-regulate themselves by adopting code of practice. The internal control is characterized by three considerations: (1) The netizens in the cyberspace could not engage in legislation activities and implement forcibly enacted rules such as constitution or law, but could only compile ethical code with sanctions limited to change and refusal of services; (2) Cyberspace is a place where inheriting inequality prevails and netizens are situated in unequal status due to their inequality before they migrated into the cyberspace; (3) Once established, the internal control has little influence on the external control, but external control has strong impact on internal control. Based on these characteristics, the decision-making process of code of practice for the internal control is hardly run with the principle of democracy and mass participation. Rather, these codes are simply drafted by one or two persons who have more concern with their commercial benefits from the service provision, with a little bit reference to the reaction and comments from the service users. The discretion is at the side of the service providers on the scale.

The external control is the order maintenance through the external mechanisms outside the cyberspace. The pure external control is where the law and order are solely imposed by the state. There is not such external control with the source of power from any other organs. When we consider the issue of external control, therefore, we are inevitable to put netizens into the web of the real society, which could in no way escape from the constraint of the law and regulation.

By saying internal and external control, we temporarily separate the cyberspace

that does not exist without the connection of information systems, from the meat space, that is, society that has existed without information systems but now integrated information systems into its territory. More safely speaking, the frontier between the cyberspace and society in the broader sense is only drawn for the convenience of this theoretical framework. Otherwise, I am strongly insisting that the cyberspace should more be regarded as the extension and an integral part of society. What are connected by information systems are the elements of this society, but not the elements of this society become independent and connected in a space of their own.

The possible forms of incorporation of internal and external mechanisms could be induced as the following:

1. Absent of internal control, absent of external control

This is a case where neither internal nor external power was installed to operated deliberate control over the order of the cyberspace. We said it is a rare case with little or no internal or external factor directly controlling over the cyberspace. But there is this kind of argument that claimed to leave the cyberspace maintained by pure technological mechanisms. This is a kind of preset arrangement, with human factors appearing far behind the appearance of their codes and programs.

Rather than case-by-case judgment over activities in the cyberspace according to existing rules, the order is maintained by preset rules that only deal with variety of situations through mechanical application of unified standard. In sum, this is a kind of technological control, with instant internal or external human elements absent. The model could be depicted as the follow figure:

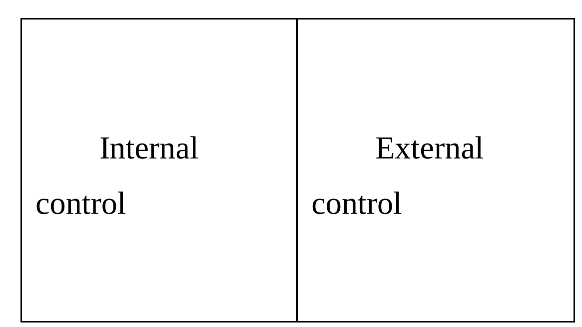


Figure 10 Absent of internal control, absent of external control

Under this model, the cyberspace was in a state of anarchy (anarchy does not necessarily mean confusion). The advocators of anarchic cyberspace claimed that the cyberspace has been created solely by technicians with technology, independent of society, free from the governing of the state, forming a new existing space. This is a

kind of space where the human relationships are in the “null-gravity state”. We can well describe it as the balance in the unbalance, the order in the disorder. The activities under such circumstances involve lower cost but take higher risk. Without any regulation and control, the Wild West metaphor of the virtual community will be the most appropriate (Many authors have exploited the metaphor of ”Wild West” about the circumstance of the cyberspace. For random examples, see Morris 1998; Clairmont 1998, pp. E1 and E2).

Due to the vacuum structure of this kind of cyberspace, the occurrence of collapse and disruption would be a sudden sooner or later. Thereafter, the attempt of internal control, motivated by desire of ownership of interests and dominative power, and/or external control, motivated by maintaining and enlarging existing interests and power, would take place. It is therefore an instable and unacceptable structure.

2. Absent of internal control, present of external control

Under this model, the internal control mechanism is not established. The order maintenance is primarily the task of the extended control from society as a whole. Although society might have different degree of democracy or autocracy, and it would naturally extend the existing mechanisms into the cyberspace, for the cyberspace, an autocracy was created with the absolute and exclusive external control, without a position of internal control, that is, through the participation of the Internet users.

This autocracy is not an autocracy in its true sense, where a society was controlled by a few people who arbitrarily exercise control over the majority. Here, the cyber autocracy was only under the pressure from outside the cyberspace, lack of any internal control mechanism.

In addition, autocracy is not one fixed model. Rather than an absolute form of autocracy, the possible forms might differ from each other by the degrees of autocratic nature. At the same time, cyberspace differs from society as a whole in the degree enjoying the control power.

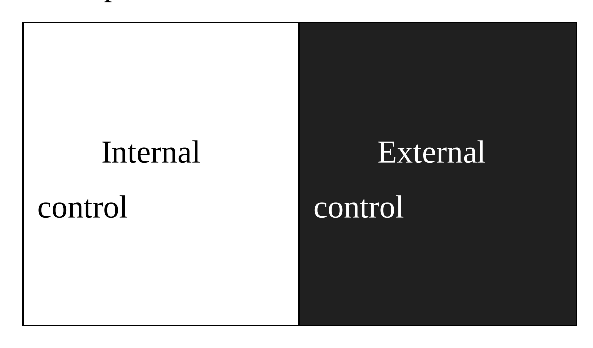


Figure 11 Absent of internal control, present of external control

If netizens enjoy few rights to organize themselves, and the government maintains the order solely, the cyberspace could be subject to higher degree of autocracy, vice versa. The current situation is that the government polices the cyberspace in the way as well as the traditional society. The rate of the cyberpolicemen to the whole population of netizens is close to, or higher than the rate of the policemen to the whole national population. Therefore, the cyberspace might become a special zone of society but not remain syncretised with the social unity.

Under such a model, the cyberspace is disciplined forcibly by the external power. For society as a whole, the activities would involve higher cost but take lower risk. However, the external control might meet with resistance from the netizens in the organized form. Again, the external control might not completely fulfil the requirements of the running of the cyberspace, which is in a sense like a well built machine. The stepping into the stage of the internal control would be unavoidable.

3. Present of internal control, absent of external control

This mode of cyberspace is organized according to the common ethics established within the online community. While ethics is needed, law is lack. On one hand, it is not possible to implement rules on the level of "law" due to the absence of the legislative power and institution. The available and feasible rules fall on the level of ethical dimension.

On the other hand, ethical dimension is relatively developed in cyberspace due to the initial independent development and self-regulation practice. The advocators of the mode believe that the ethical mechanism can work well keeping the cyberspace into order. The netizens under this model constraint their own behaviours according to the ethical code of the cyberspace, avoiding from the breach of the cyberspace, and from invading society. However, the internal control might be confronted with the risk of breakdown due to lack of forcible enactment of sanction, and thus induced is the outside interference, that is the filling-in of the external control.

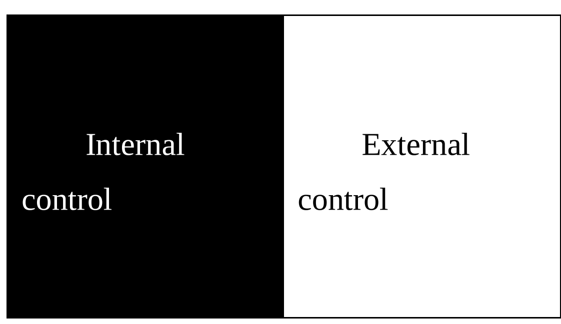


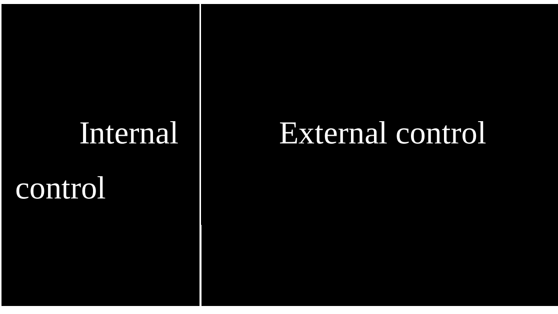
Figure 12 Present of internal control, absent of external control

4. Present of internal control, present of external control

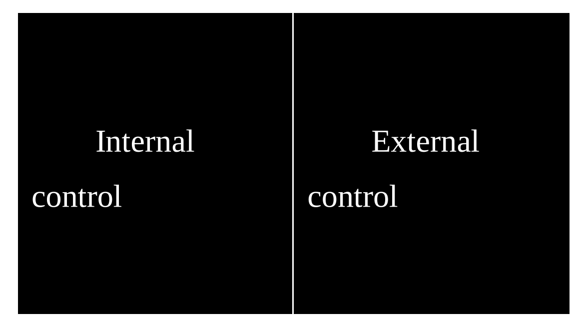
By the fourth model, we are seeking to balance between the external control and internal control. Both internal and external control would play roles in the order-maintaining process. This includes a series of balance such as between internal factors, between external factors, and between internal and external factors. The model includes both a certain degree of internal control and a certain degree of external control, in which the activities might involve higher costs but take medium risk.

The creation of this dual control could either be a result of compromise between the desires of cyberspace as an integral part and as an autonomous zone of society as whole on one hand, and the other parts of society; or be a result of conspiracy between some of the netizens and the other part of society. Regardless of the nature of such compromise or conspiracy, despite the continuous change of balance between powers of internal control and external control, this is the most possible and stable model, be it not within the ideals of many acclamations.

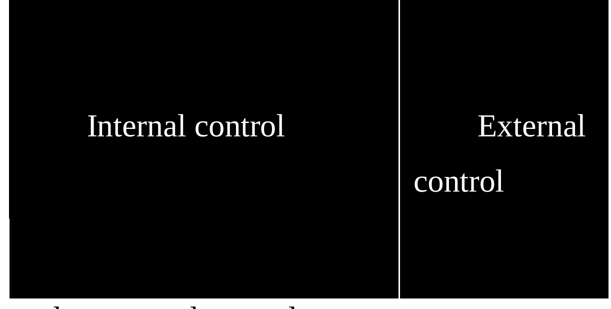
The leverage in this model could move from the left to the right, that is to say, the degrees of internal control and external control could differ from strong and weak. In some case as depicted in Figure 5 (1), the internal control is weaker but the external control is stronger with the leverage located in the left part deep into the frontier of the internal control. In Figure 5 (2), the internal control and the external control are ideally balanced with the leverage located on the medium frontier between internal control and external control. In Figure 4 (3), the internal control is stronger but the external control is weaker with the leverage located in the right part deep into the frontier of the external control.



(1) Internal control < external control



(2) Internal control = external control



(3) Internal control > external control

Figure 13 Present of internal control, present of external control

We can hardly draw a conclusion on which model is the beneficial or practical. It is a question of which discourse is the dominant. There are those who advocated the cyber anarchy, leaving the cyberspace as it is, resisting any artificial control either from inside or from outside. Yet their voices have been too weak to be heard by the netizens and non-netizens. Particularly, society's prevalent discourse might not be compatible with an anarchist view. The same is in the cyberspace. Many also argued for solely internal control over the cyberspace, denying the externally imposed state arrangement. However, in this case, it is not words, grammar and reasoning that are functioning. It is the legislature, police, court and jail doing so. Therefore, solely external control rather than solely internal control is more proximate to the goal of the order of the social unity.

Given neither absolute internal control nor absolute external control is possible,

the more acceptable and more stable structure of cyberspace order might be under a mechanism in which the cocktail of internal control and external control is mixed. It is as if the cyberspace is a globe, which the gravity attracts the elements and materials towards the core, while the outside pressure condenses its cubage. As a result, cyberspace exists in a form of a dwarf star, only in which form, cyberspace becomes an integral part of society as a whole, with a stable and acceptable order.

The risk of the hypothesis of formal rationality together with computerized justice system

Modernity of law was supported by many ideal ideas of which formal rationality is one most recommended by the enlighten thinkers, and one most criticised by the postmodernist advocators. The ideal of formal rationality believed that rule of law could be achieved, given goals such as systematization of legal system, installation of professional jurists, well arranged process, etc.

The use of the powerful computing machine in the latter part of the last century became an incentive for those who insisted that formal rationality could be achieved with the help of the mechanical calculation of the elements of mens rea, actus reus, due process, equal protection, etc. Their inevitable operations have been to quantify both the quantitative and the qualitative factors with the tools of pinch cards, sentencing guidelines and computer software.

Ironically, the coming of the idea of computerized justice system roughly coincided with the initiation of the postmodernist criticism against the blankness of formal rationality. The phenomenon could well be conceived as a hidden form of resistance of the despairing ideal of rule of law against the possible adaptation to the changed social environment. While legal retrieval system is a beneficial element in impelling subjects to be more informed of the certainty of the law, the computerized justice system might pose a hindrance by maintaining the conventional order on the contrary direction to the former.

In all accounts, mechanical computerized justice system is not akin to the postmodernist legal studies. It is a misplantation if there is such a discourse as to incorporate such different creatures in the macro-environment where what happened simultaneously is prone to be considered of same features. In doing such logic reasoning, the balance of linguistic powers out of the opposed fronts is inevitable and unfortunate.

The use and abuse of information systems in doing law and doing legal studies are happening abundantly in current time. But the divarification of the use and abuse would come into being sooner or later. This is to abandon the seemingly reasonable but practically unreasonable ideas, divulged from the prevailing information systems facilitated legal discourse. Thus the clarification of role of mechanical computerized justice system and the like should be given first priority in addressing informed legal order of society and its extension into cyberspace. The time when everything could be hidden behind this information curtain and appear with this fashioned mask would come to an end, together with the dream of mechanical computerized justice system. Information systems, in fact, cannot do such a thing as doing law. The basic questions such as “who would write codes and compile law into such a program?” and “who would sit at the desk to finger keyboard to operate such a system?” cannot even get logic answers without refer to the outdated ideals.

Conclusion

The change of legal system in the environment where the pervasive use of information systems forms an irresistible force in shaping nearly all lives of society needs specific attention. The discussion above briefly defined the limit of its boundary. While we have the very reason to exclude the so-called virtual space from the current field, we make no attempt to negate the value of further inquiry into the all the unique respects brought about by the development and understanding of the new technologies, which in turn indeed leads the old legal thinking up to a novel platform. It is on this higher level that the hypotheses of improved legal literacy and informed rationality operate. The essay's other objectives are to construct the models of order in cyberspace over which internal and external forces exercise control to varying degrees. Although the information society in general and the cyberspace in particular is designed toward an environment accommodating a more ideal legal system, mechanistic calculable justice standard would not be realizable in an optimistic future.

References

Bartle, Richard A. 2004. Pitfall of Virtual Property. Retrieved 14 January 2009, from http://www.themis-group.com/uploads/Pitfalls%20of%20virtual%20property.pdf

Clairmont, Susan. 1998. Police Compare Cyberspace to the Wild West and

Dangerous, *The Hamilton Spectator*, 14 August, pp. E1 and E2.

Dibbell, Julian. 1993. A Rape in Cyberspace, *Village Voice*, Volume 38, Number 51, 12 December. Retrieved 14 January 2009, from http://www.ludd.luth.se/mud/aber/articles/village.voice.html

Durkheim, Emile. 1933. *The Division of Labour in Society*. Glencoe: The Free Press.

Fairfield, J. 2005. Virtual Property, Boston University Law review, Volume 85, pp. 1047-1102.

Hobbes, Thomæ. Malmesburiensis opera philosophica quæ latine scripsit omnia, Vol. II, Londini: Apud Joannem Bohn, 1839.

Hobbes, Thomas. 1962. *Leviathan*, New York: Collier.

Mason, Moya K. (ed.) 1998. Bibliography, in Howard Rheingold, *The Virtual Community*, 2nd Edition. Retrieved 14 January 2009, from http://www.rheingold.com/vc/book/biblio.html

Milovanovic, Dragan. 1994. *A Primer in the Sociology of Law*, 2nd edition, New York: Harrow and Heston Publishers, pp. 40-47.

More, Thomas. 1989. *Utopia*, Cambridge: Cambridge University Press.

Morris, Andrew P. 1998. Feature: The Wild West Meets Cyberspace, *The Freeman: Ideas on Liberty*, Volume 48, Number 7.

Paine, Thomas. 1844. *Common Sense*, Dedham, Mass., re-printed by H. Mann for S. Bryant, esq.

Plato. *The Republic*. Retrieved 14 January 2009, from http://www.gutenberg.org/dirs/etext94/repub13.txt

The Twelve Tables. Retrieved 14 January 2009, from http://www.fordham.edu/HALSALL/ancient/12tables.html

Weber, Max. 1978. *Economy and Society: An Outline of Interpretive Sociology*, Guenther Roth and Claus Wittich (eds.), Berkeley: University of California Press.

Chapter II Exploring into Regulatory Mode for Social Order in Cyberspace

Abstract

An increasing necessity for building cyber order through legal instruments has existed as one of many alternatives to regulate the world dominated by the globally connected Internet. While cyberspace is global and cyber-activities have remote reach, laws, which are different from one country to another, have been historically designed to deal with acts occurring within territorial limitations. For several years, numerous explorations into possible arrangements, from super-national, international to national laws in separate countries that can possibly be applied to maintain cyber order have been flawed in balancing interests of users and regulators of different jurisdictions. Traditional spatial divide between jurisdictions has been precisely transplanted into cyber-laws. This article discusses legal gaps of cyber-laws among different localities, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. The official action must be within the ability of the controller so that it can be effective, and that it must also cope with the utility of the controller so that it can be efficient.

Keywords: cyber order, regulation over cyberspace, ability-and-utility-oriented control (AUOC), steps in data movement

Introduction

Information and communications technologies (ICTs) come from and have significant impact on society. Many human activities with functions and patterns different from that of traditional society have been facilitated by the globally connected computer networks. Previous ethical and legal discourses are undergoing serious challenge from newly emerged cyber-semantics. If we are going to set a limit between meanings of cyber- and traditional activities, there can be found some

clearly defined, however controversial, characteristics. The conundrum happens when organisers of society have the same interests in guaranteeing the successful expansion of their immanent regulatory instruments from traditional society into cyberspace without a loss in enjoying their existing power. Nothing would be tolerated in case it is simply an activity that takes place in cyberspace, other characters being the same as that in the meat space. We can perceive some particular cases as exceptions; however, they can only be seen as exceptions to the mainstream tendency. It could be well expected that online behaviours would have no more difference from their offline counterpart in respects of getting regulatory results.

For some time, cyberspace enjoyed some extent of happiness from evading regulation as strict as on the traditional society. A variety of negative effects emerged and countries have growing eagerness to include activities in cyberspace into their jurisdictions. Nevertheless, a string of impediments deferred the process of integrating online and offline "activities". All countries are territorial-dependent, and no on single country has ever had claimed global control over all humans in the world, with rare exceptional situations where some countries extended their jurisdictions beyond their territories by domestic legal acts or according to international agreements. The networks-facilitated cyberspace has a virtually global reach in the sense of spatial concept, exactly going beyond single countries and in a certain sense incurring the ardour of countries to exercise control over it by one ultimate entity: a country, or an institution. However, it has never come true that a universal jurisdiction principle is accepted as a general rule in either meat spcae or cyberspace. Academia, legislature, and law enforcement agencies have all been devoted themselves to harmonising domestic laws or meliorating international laws in order that they are applicable to cyberspace in conformity with meat space.

Furthermore, cyber-activities have innovative players, processes, and objects. The new players are netizens hooked online through wire and wireless links, acting through transmitting digitalised information, and influencing status of objects without physical appearance in person. The identity of the players can easily be concealed, the trace of their activities be eliminated, with their locality impossible to be spotted. Adding to these complexities are perplexities that even if they are identified they can still be involved in legal controversies, either that their activities regarded as legal by one country are denounced in another country, or vice versa.

We expect that the core arguments in this article concerning the approach to

online content can also be useful in dealing with other online legal questions, such as unauthorised access to information systems, piracy of intellectual property, fraudulent schemes, destruction of data, defacement of websites, dissemination of malicious programmes and so forth. All these online activities with negative social evaluations have generalities in common, even though there are also many particularities. That is because of similar extent of social evaluations on these obnoxious activities that make countries to motivate their legal instruments to tackle them. Of these activities, online content has been one of the most controversial issues, over which many countries make efforts to exercise control. From the point of view of regulators, it is an urgent task to discover a route for installing previous rules in cyberspace regulation.

In determining the optimal selection from a variety of regulatory alternatives based on national orientation in cyberspace, we should first examine advantages and disadvantages of each option and reason which one has the highest meritoriousness capable of dealing with jurisdictional effectiveness and pecuniary efficiency.

Structure of the reasoning

Regulation of cyberspace has attracted great attention from academia since late 1990s. Many people have invoked laws of different countries for or against regulation of cyberspace. Therefore, there have been significantly different standpoints concerning whether cyberspace should be regulated, and if we give a positive answer, to what extent it should be regulated. In particular, online content may be the most controversial respects of such a disputation. In the U.S., for example, freedom of speech has been established on a firm constitutional foundation through its First Amendment. Oftentimes it has been interpreted in a broader way than many (if not any) of free speech provisions in the world. In China, for another example, both governmental and civil views, which usually distinguish between content considered legal or ethical and content considered illegal or unethical, are in favour of some kinds of regulation over online content (Fallows 2008). Even though people from the U.S. may assume that control of the Internet in China might be an unhappy experience, majority of Chinese netizens seem not so resistant to such a way of control (ibid.). This fact indicates that different attitudes do not obstruct us from discussing ways of control.

This discussion is based on the assumption that some kind of regulation over cyberspace should be imposed, regardless of the extent to which such a regulation should be. Lessig's code approach (Lessig 1999) has (over)stated the role of code as a potential regulator (a subject, or a tool?). Kerr's perspectives approach (Kerr 2003) attempted to bridge the gap of understanding between cyberlegal problems and conflicts between internal and external perspectives. Weiser's competitive platforms approach (Weiser 2003) assigned each of cyber processes to a certain layer. Rather than calling them layers, I would simplify these aspects as nodes that comprising the whole chain of data movement. In practice, some others also mentioned different stages of data movement, such as Zittrain (2003), who divided the process into five stages: from source, to source ISP, to cloud, to destination ISP, and to destination. However, my typology would consider not only stages of data movement but also intervention of human elements with mechanical transmission and processing. In so doing, data movement will be considered as beginning with human intervention with mechanical transmission, without which no data can be input and no command can be sent for data processing and transmission. In this step, human intervention is a necessity for commencing the data movement through human-machine interaction. It is the human entity at the starting point of the run initiates the whole process, whatever the effect will take place. Subsequently, data movement will be realized in a step when human intervention is not a prerequisite but it can still be possible that human intervention is involved. This step is symbolised by machine-machine interaction, with or without human intervention. The third and last step ends with machine-human interaction that has impact on human entity at the destination. Here we use the term step instead of period, phase or stage by considering that the duration of the process of data movement is rather short, and that the beginning and the ending of the process are more like two temporal points than two periods. The only longer duration happens in between these two ends, that is, the movement itself, which is also rather rapid and instantaneous. People use such term as "synchronal," "synchronic," "synchronous," or "synchronized" to describe such a situation. Thus we establish a typology including three distinct steps in data movement: human-machine interaction step (HMIS), machine-machine interaction step (MMIS), and machine-human interaction step (MHIS).

Control at human-machine interaction step (HMIS)

Human always predominate data movement. But human also play different roles in data movement from the beginning users through deposition, hosting, transmission, and processing by machine to the end users. At human-machine interaction step of data movement, human acts more predominately than in other steps. It is these activities with predominate nature that primarily determine the human involvements at other steps, let alone mechanical involvements and human-machine interaction.

As far as online content is concerned, players at this step include online content authoring parties (OCAPs) and online service providing parties. OCAPs are those both individual and institutional users who write, create, demonstrate, perform, record, upload, review, publish, distribute, disseminate, propagate, lease, lend, sell by wholesaling or retailing, or have the content to enter the movement process by other means so that it can reach other users. Apparently, players at human-machine interaction step act more actively in putting data online. Besides authoring parties, online service providing parties are also involved in the initiation of this process by accommodating movement of content-related data.

Eliminating incentive of OCAPs may be the most effective option to exercise control over online content. If and only if potential authoring parties could no longer benefit, either financially or spiritually, from authoring, online content would no longer be authored. Thus the most effective control begins with control over authors. However, this effectiveness can not directly be translated into efficiency due to the geographical distribution of global users. Authorities are simply confronted with jurisdictional limits based on international political borders. Law enforcement is still operated in a rather conventional way that is reluctant to positively face jurisdictional conflicts, which is deepened by ideological, political, ethical, legal, procedural, methodological, and technical conflicts. As a result, to discourage authoring parties by various possible ways become an unfavourable idea.

Yet worse, once motivated authoring parties upload the content online, it is published to a media with a global audience and delivered on a nearly hybridly regulated platform. Even if the purpose of regulation is not for penalty itself, once spread, online publications can not simply be removed thoroughly. The existence and dissemination of such content become an eternal digital movement.

Now we have to turn to Internet service providing parties (ISPPs) who have

certain ability to control data movement, even though their functions are originally not limited to do so. ISPPs may be immune from any liability in many situations, but they are imposed some kind of liability in some other situations. If we stop at discussing this issue only at the layer where ISPPs are supposed liable, it is a typical *mala prohibita* if ISPPs are imposed liability for their failure in fulfilling responsibilities that authorities would possibly assign to them. Because they are located in a condition where it is more possible to exercise control over online content authored by others, to assign them certain responsibilities, failing to fulfil which will be punished, is economically and judicially a more efficient way than attempting to prosecute authoring parties that are jurisdictionally impossible to prosecute.

ISPPs are usually more established, more organized and more centralized entities than authoring parties. They are more likely to act anonymously than single individuals and institutions. They are also likely to operate with more stable localities. These characteristics render ISPPs a status that the regulators can use to remove unfeasible content and even launch legal actions against ISPPs themselves.

ISPPs are not only passive in accepting authoritative commands, but they can actively exercise control over content within the scope of their services. For example, they have the capacity to take measures to direct content to where it is acceptable and avoid directing them to where it is unacceptable. In other words, ISPPs have much say on data movement: whether data move, when data move, where data move, or to whom data move. Thus, control over OCAPs can well be translated into control over ISPPs.

Control at machine-human interaction step (MHIS)

Online content consuming parties (OCCPs) are end users of data movement in the case of content-related transmission. They have both similarities with and differences from OCAPs in data movement. While OCAPs start up the process of data movement, OCCPs put the process of data movement to an end, ending in consuming: either downloading, reading, watching, listening, using, enjoying, borrowing, renting, redistributing, re-disseminating, or re-propagating, but mainly for their own consumption. Even though OCCPs as end users engage in passive acceptance and active mining of online content products (OCPs), their activities are

passive in nature. If there is no online content existing for their consumption, these end users could never reach such OCPs in online content market (OCM). Thus it is a reasonable option for interest authorities to restrain their impulse to exercise control over activities of OCCPs. In particular, authorities of one country reluctantly have the motivation for impose certain liability on OCCPs in another country. Territorial jurisdiction stops before the borderline between countries.

It has never been a good idea to exercise jurisdiction on persons living in other political entities. The computer networks did not change the traditional concept much. Even if some people attempted to broaden the understanding of authoring activities to the extent that it covered the actual activities of reconstructing digits into complete files through downloading, viewing, browsing, retrieving and saving in magnetic media, they are increasingly put to an unfeasible place serving as the synonyms of “authoring” or “possession”. The applicability of rules against possessing or authoring such online content cannot be uncontroversially justified. Otherwise, to control individual and institutional OCCPs is confronted with the virtually same predicament as in the case of OCAPs: they are just similarly distributed in a geographically global space and control would be inefficient and ineffective. Morally or legal preventing such contents usually give place to technical measures, which are gradually invented to arm authorities all over the world to filter content that they separately classify as objectionable according to their own standards.

It happens that it is difficult for authorities to directly regulate each and every OCCP, and that there are also nodes directly serving end users. That is those nodes that have to take responsibility for controlling activities of OCCPs and those who fail to do so would be held liable for the unfavourable consumptive activities involving retrieving of objectionable online content. Similar to ISPPs at the starting point of data movement, ISPPs at the end point of data movement also become the targets of authoritative regulation, for the sake of efficiency and effectiveness. ISPPs are neither end users nor regulators, but become controllers of end users and controlled by authorities. That’s why ISPPs are usually not willing to orientate themselves as located in between end users and law enforcement.

Control at machine-machine interaction step (MMIS)

Control over activities of start uses and that of end users in the chain of data movement with special regard to online content market proves problematic. Extended control over ISPPs that are adjacent to star and end users can partly be justified. Because there are altogether three steps in the process of data movement, we must now clarify the controllability of the interstitial step.

Quite a lot of players live on digitally linking start and end users. At this step, human elements are automatically played down by deep involvement of technological and technical solutions. Technologically, portals and search engines attract and facilitate users to harvest online content. Human there have technological means to provide some kinds of options for data movement. Obviously, machine-machine interaction is in practise dependent on regulatory direction from human, who receive another level of regulatory direction from authorities.

The possibility of human intervention through technological and technical measures at the step of machine-machine interaction of data movement does not automatically mean that it is easy for portals and search engines to filter and prevent large quantity of moving data. In fact, imposing liability for omission to filter and prevent objectionable online content would be less efficient and effective than imposing liability for commission to providing hyper links. This exactly is where the responsibility and liability should be placed. Creating an incentive for human interveners to bear a burden for doing something extra would not be work better than creating an incentive for them not to do something unfavourable. To move somebody doing something extra beyond their duty while no compensation is provided, she/he would manifest some kind of inertness in reaction. In case of punishing somebody for doing something objectionable from the point of view of government, she/he would present a higher degree of coordination. Purpose of regulation is just located in coordination but not punishment. In designing a mechanism to subject human elements to coordinative data movement, OCM would be operated following its orbit of economic utility. In sum, human interveners at the machine-machine interaction step have certain degree of ability to exercise control over data movement by bearing additional of filtering and preventing data but have less utility to do so. On the contrary, they would have both ability and incentive to exercise control by not providing access opportunities for certain data.

Ability-and-utility-oriented control (AUOC)

Our analysis on regulation and control at different steps of data movement reveals that the official action must be within the ability of the controller so that it can be effective, and that it must be also out of utility of the controller so that it can be efficient. On the contrary of this conclusion is that control by controllers without ability will be ineffective, while control by controllers without utility will be inefficient. Only control by controllers with both ability and utility will be effective and efficient. Based on this principle, only local authorities who fall in the same jurisdiction as where players who play negatively are located may actually exercise control over relevant step or steps of data movement. Those authorities without interest in affairs that players play negatively are monetarily discouraged from exercising control.

The logic in online content market is that, those who are able to exercise certain extent of control, who are assigned the responsibility for control and who fail to exercise due control would be held liable. These players seem to play in a broad "online" ground. However, when responsibilities are assigned to players, they do not simply mean to do something in favour of authorities. On the contrary, they sometimes simply mean not to do something unfavourable to the authorities or society. In other words, omission is not taken into account when liability is imposed, but commission renders the players into perfect liable status if such commission leads to data movement that disseminates objectionable content to OCCPs, who without such commission would not have access to such content, or who without such commission would have less numerous, frequent, or convenient access to such content.

However, ability is a must in considering to whom the responsibility should be assigned. To assign responsibility to players in a status unable to fulfil, would make it morally unjustifiable to hold them liable in law enforcement stage.

Control over online content market has to be exercised in a way balance ability and utility of concerned players. Ability only or utility only is a vacuous design of regulatory framework. Taking both of them into consideration would avoid dilemmas in justification, and efficiency and effectiveness.

Control over online content is neither designed to exclude as much users from the OCM, nor to prevent as much users from the beneficial consumption of content. Utility is a must in considering mechanism for control. To assign responsibility to

players in a status unbeneficial, would make it economically inadvertent to move them fulfil their responsibility.

Conclusion

Traditional spatial divide between jurisdictions has been precisely transplanted into cyber-laws. Legal gaps of cyber-laws among different localities survived, nevertheless. This paper explored a control model, which can be called ability-and-utility-oriented control, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. The official action must be within the ability of the controller so that it can be effective, and that it must be also out of utility of the controller so that it can be efficient.

References

Fallows, Deborah. 2008. Few in China complain about Internet Controls, March 27. Retrieved 14 January 2009, from http://pewresearch.org/pubs/776/china-internet

Kerr, Orin S. 2003. The Problem of Perspective in Internet Law, Georgetown Law Journal, Volume 91, pp. 357-405.

Lessig, Lawrence. 1999. Code and Other Laws of Cyberspace, New York: Basic Books.

Weiser, Philip J. 2003. The Internet, Innovation, and Intellectual Property Policy. Columbia Law Review, Volume 103, pp. 534-613.

Zittrain, Jonathan. 2003. Internet Points of Control, *Boston College Law Review*, Volume 44, Number 2, pp. 653-688.

Chapter III Legal Roles of Information Systems

Abstract

In this article, information is classified according to its value into five categories, including information with positive value, value-neutral information, valueless information, information with negative value, and information that its value is disputable. The article further analyzes the interaction between information and criminal law, particularly the necessity for criminal law reform in the information age.

Keywords: Classification of information, legal roles of information systems

Introduction

After the introductory text of this article, I am now going on to discuss the subject-matter in detail. The following text will deal with the conception and classification of information in the domain of law, and the challenge it poses to the traditional legal system.

When we explore society, we begin with observing human beings ourselves. Human beings have a determination of orientation to survive and to front the uncertain, unstable and uncontrollable environments, both physical and social environments, whether natural, constructed or cyber. It is this orientation to survive the uncertainty and to know the unknown that propels human beings to reshape the already shaped, reconstruct the already constructed, and reorganize the already organized.

It has long been recognized that both nature and society are changing. What Heracleitus said "One cannot step twice into the same river," (Heracleitus 1979, p. 168) can be understood broadly as recognition of a changing world. The present day idea of change is accepted as the inherited nature of existence. While the discussion here will not be reduced to philosophical assertion, I accept that change is the eternal attribute of society. Accumulation of information contributes greatly to social transformation. Digital information has become the decisive innovative factor in economic

development and the leading resource in contemporary civilization (Molitor 1982, p. 84; Fisher 1984, p. 1; Rabin and Jackowski (eds) 1988; Daler and co-workers 1989, p. 13). Just as good land is a decisive factor for the agrarian economy, capital for the industrial economy, existing knowledge is a decisive factor for the information economy (Stonier 1983, p. 21). The relationship between these factors is not simply parallel, but progressive. In contrast to land, capital and information are more closely linked to human interactions. In contrast to land and capital, information is more closely linked to interactions of human intelligence. To say their relationship is in a progressive style is to say that information is the newer and higher level of achievements of human efforts (See Table 1). The implication of the recent information revolution lies in the fact that it is designed to eliminate the shortage of knowledge by processing data and information.

Table 1 Land, Capital and Knowledge

Factors	Land	Capital	Knowledge
Forms of the economy	Agrarian	Industry	Information economy
Forms of interaction	Non-interaction	Human-human interaction	Human-machine-human interaction

Information is therefore the enormous wealth of the social progress, which has been considered the fourth resource (UNCJIN 1999, Paragraph 85), alongside natural resources, property resources, and human resources. In contrast to other resources, information can be regarded as the only resource that can really be shared (Stonier 1983, p. 19). Fisher used a metaphorical statement describing information as power, “power to manage, power to manipulate, power to control” (1984, p. 1). Tapscott, Ticoll and Lowy (2000) further discussed the conception of digital capital in terms of business, stating that digital capital emerged from the incorporation of three types of knowledge assets: human capital, customer capital, and structural capital (p. 5). With the network, people could “gain human capital without owning it; customer capital for complex mutual relationships; and structural capital that builds wealth through new business models.” (ibid.)

Other scholars further put information into a dynamic wealth-creating process, regarding information (particularly knowledge) a “key wealth-creating assets” (Porter

and Read 1998, p. 26) apparently in a dynamic productive and reproductive process. Information processing is thus a process of promoting social productivity.

Unquestionably, the traditional resources have been seen as incomparable with the capacity of information, which can bring about enormous productivity and unprecedented social transformation. Information and related technology has created a new epoch, a new society, and a new way of thinking for the modern human beings. In our reading of traditional society, one thing stands out as fundamentally different from the information society, which is information dependent, information abundant, and information shared. Bjørn-Anderson and co-workers (1982) correctly predicted that the information society would be characterized by the remarkable increase of information flow, the contraction of temporal and spatial constraints, the increasing dependence of social life on information systems, and the synchronous application of new technology on society (pp. xi-xii). It is apparent that people consider information as being of positive value and grant potential power in its conceptual category.

People usually distinguish information from both data and knowledge. According to Stonier (1983), data is a series of unconnected facts and observations, likely to be changed to information through refining or organizing activities, while knowledge is organized form of information, providing the basis for insight and judgments (p. 19) Detailed relations between the terms can be illustrated as in Figures 2 and 3. On the other hand, information at one level may merely be data at another level (ibid). Finally, there can never be a clear limit between these terms. They are usually used interchangeably. For example, knowledge is the highest level of data or information, but people do not talk about knowledge security instead of data security and information security. In addition, information systems are actually "data systems" (See Johnson 1970, p. viii), but the favourite term in various disciplines is still "information systems". In this study, the word "information" is priority choice where these three words can be used interchangeably.

In sum, the strong and the wealthy in the agricultural society strive for more and better land; the strong and the wealthy in the industrial society strive for more and better capital; and the strong and the wealthy in the information society strive for more and better information.

Nevertheless, the term "information" is theoretically used as a value-neutral term. From the viewpoint of law, the term "information" stands for "data, text, images, sounds, mask works, or computer programmes", including the process of

collecting and compiling them (Uniform Computer Information Transactions Act (UCITA), Section 102 (35)). Important elements involved in defining information in the modern sense include:

Information is electronized. The current processing form of information is characterized by mobilization through electricity, fastest known vehicle.

Information is digitalized. The current information is processed in the form of digits, “0” and “1”.

Information is computerized. Information is created, deposited, processed and transmitted by the assistance of computer, a powerful “information machine” (Konig 1967, p. 1).

Information is automatized. The process in which information is created, deposited, processed and transmitted is a kind of human-machine interaction. There is no absolute automitization.

Information is networked. Information is transmitted through the networks. It is electricity, digits, computer and automitization that constitute the basis of the networks.

Information is modernized. It is not in a process of modernization, but in a process from modern to post-modern. It is modernized thus transformed. The change breaks the equilibrium of the conventional control and organization, motivating somebody to harvest from deviant actions, exposing somebody else to potential threats, and reducing the effectiveness of any safeguard.

Information is evaluated. The value of information is recognized, accepted and respected.

Lacking any of these elements, the object can hardly be regarded as information. The modern definition of information therefore inevitably contains different factors from the traditional meaning of this term. Many people nonetheless misunderstand the exact meaning of information and consider that law has regulated information for several centuries or millenniums. This suggestion ignores the difference between information in the traditional sense and that in the modern sense. While the traditional form of information is heavily substance dependent, the modern information is processed by digital technique. The present information is practically transformed into digital information, regardless of whether it ever existed in the pre-computer era. Particularly, on account of the specific form of existence, a copy of information is not necessarily different from the original information in content,

quality and medium. Under such circumstances, the term “information” can precisely cover a copy of information Uniform Computer Information Transactions Act (UCITA), Section 102 (10)). In the network environment, information, its copies, and the copies’ different digits may be transmitted along the cable, fibre, or wireless networks without the spatiotemporal limits.

Considering the different roles of different categories of information in the legal system, it is necessary to classify information according to its value from the standpoint of law. Law does not provide equal protection for all kinds of information. On the contrary, law merely encourages the processing of information with a positive value, but discourages the processing of information with a negative value. Although people deem information systems to be part of a critical infrastructure, and we transmit various kinds of information through the same information systems, the legal nature of these kinds of information should be differentiated.

Classification of information in the legal sense

Social inquiry usually starts from conceptualization (Babbie, 1995). Having talked about the conception of information, and not necessarily repeating accepted definitions, this section will give a sketch of classification.

The legal value of information has long been recognized (See UN Recommendation on the Legal Value of Computer Records, adopted by the Commission at 18th session 1985). The legal effect, validity or enforceability of information should not be rejected simply on the ground that it is in a form different from that seen in traditional documents (Article 5, Model Law on Electronic Commerce of the United Nations Commission on International Trade Law, Annex of General Assembly Resolution A/RES/51/162). As in United States v. Adajan case the court ruled that computers could be at the same time storerooms of private information that must be guarded, or that of criminal proofs that must be identified (United States v. Christopher Lee Adjani; Jana Reinhold, No. 05-50092 D. C. No. CR-04-00199-TJH-01 OPINION, 13 January 2006).

Previously, people were inclined to dichotomize information into legitimate and illegitimate, for instance, Sterling (1994). The nature and content of information are far broader than merely being legitimate and illegitimate. The value of information can be regarded as a criterion for a typology. On this terrain, information can be

sorted into five categories according to the value it has and by whom it is held: information with positive value, value-neutral information, valueless information, information with negative value, and information with disputable value in different communities.

The first category of information, information with positive value has the capacity to promote social welfare. The positive value of this category of information depends on the content of the information. If the offenders access to or destroy such information without authorization, the value of that information would be abused or exterminated. Loss of information with positive value, or loss of value of such information, either due to breach of its confidentiality, integrity, or availability, diminishes the efficiency of the information owner or, in turn, promotes the efficiency of the opponent. Offences involving infringement of information with positive value, infringe the rights and interests of the information owners. The related acts include unauthorized acquisition, modification of, destruction of, and tampering with information, and interference with information transmission. In particular, offences related to the ownership of information may possibly infringe the rights to information, such as appropriation, unauthorized use, obtaining income, and disposition. To copy, retrieve, deposit, publish, duplicate, utilize, promulgate, transmit, conceal, encrypt, decrypt, transfer, sell, etc., without authorization or legal permission, are all conducts that can breach the ownership of information.

The second category of information, value-neutral information indicates that the value of information cannot be classified into positive or negative. Rather, it can be utilized as either positive information or negative information, or used as positive information or negative information. This kind of information can neither automatically advance social prosperity, nor necessarily impair social interests. This kind of information can be either used or misused, or simply exists in itself. For example, collections of e-mail addresses can be used in sending advertisements of opt-out electronic marketing, or fabricating an advance-fee scheme. However, these addresses are value-neutral, as the user names and passwords are, too. This category of information is value-neutral from the standpoint that its content cannot be judged to be positive or negative as such.

The third category of information is valueless information. Some information has no value, for example, unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE) without information of either a positive or negative value. The

distinction between value-neutral information and valueless information lies in whether the value-neutral information does not induce a question of value judgment, and people cannot evaluate it as favourable or unfavourable; while valueless information induces value judgment, and people can evaluate it as neither favourably, nor unfavourably, but ordinarily as futile. In contrast to value-neutral information, valueless information can be used neither to promote social welfare, nor to degrade the social interests. This category of information is valueless by virtue of the fact that its content is valueless. However, the process may impair the normal order of the cyberspace by disseminating and transferring such information through information systems with malicious intent. The transmission of the valueless information exploits the bandwidth, forming a worthless data flux and wasting the receiver's time to deal with it. If the fact is of high ambiguity, the users have to spend time to browse around the information; even if the matter is of high certainty, the users also have to spend time removing the information. Even though each user wastes merely a few seconds or minutes, the time wasted by millions or even billions of users will be a substantive quantity. The process will virtually diminish the efficiency and increase the expenditure.

The fourth category of information, information with negative value indicates that the appearance, existence, and dissemination of information are detrimental to the stability of the state, public order, and individuals. It does not exist without the intervention of human factors. Some are created with malicious intent, for instance, a computer virus; some are created from a contradiction within one's value concept, in which he or she regards it as legal and beneficial to deal with such information as adolescent pornography, hate speech, etc.; some information is falsified information, fabricated with the purpose for defrauding and obtaining property or other benefits, or for disparaging, defaming, blaspheming, etc. To reproduce, sell, promulgate, publicize such information are all measures that cause monetary losses or other damage to others.

The introduction of negative information into information systems poses a series of risks that may lead to perilous and erroneous decisions, and cause impairment, suicide, and calamity. The risk of these threats necessitates an increasingly higher level of cybersecurity guaranteed by diverse specific services, with increased expenses and personnel. The entire society, from individuals, organizations to governments have to deal with the misinformation, manipulation of public opinion,

and onslaughts against the social order and interests.

It is necessary to note that information with negative value can be converted into information with positive value once that information is recorded and stored by judicial agencies as evidence to hold the fabricators and disseminators liable. This does not indicate that the value of information changes, rather, that the information is used to prove the existence of the *actus reus* by its specific negative value. It is necessary for success in the prosecution of crimes related to information with negative value to seize information as evidence. The application of evidence rules should not pose any obstacles for the admissibility of information as evidence (Article 9.1, Model Law on Electronic Commerce of the United Nations Commission on International Trade Law, Annex of General Assembly Resolution A/RES/51/162). It should be granted because of its evidential weight (ibid., Article 9.2). Therefore, information should be differentiated in both substantive criminal law and criminal procedural law.

Besides the above four categories, there is a fifth category of information the value of which is disputable in the legal sense. That is to say, the criteria for evaluating the information are different in different countries. For instance, in some countries adult pornography is protected as free speech by the constitution and other laws, while in other countries its creation, production, duplication, publication, transaction, and dissemination are strictly forbidden. Furthermore, information can constitute a kind of political propaganda, which is also granted a different legal position in different countries, some having a high degree of free speech, and others having tight laws of political libel, and so forth.

Although information can be distinguished according to subjective judgment, it does not in itself represent virtue or vice. The pervasiveness of information does not constantly push forward social development and facilitate the maintenance of the legal order. Through technological supremacy, all kinds of information play certain roles, exert their influence, and gain markets. They are all regulated, intercepted, and monitored. Similarly, they all bear the risk of unauthorized access and destruction. In addition, it is possible to obstruct positive information by legislation and court rulings, while negative information may be protected erroneously. Accordingly, information products and services, sources and destinations, storage and flux, domestic and international information, and public and credential information bring about the complicated process of value judgment. In this dissertation, except when otherwise mentioned, the term “information” is used in a positive sense.

The full power of information has been realized through ICT, which has a broad impact on social lives, including maintaining the common traditions through improving the accessibility of information about religious practices; keeping cultural continuity through access to more information; enabling governments, commercial businesses, news and media organizations, as well as educational organizations to perform their functions well; and increasing collective activities and interests through an improved work process and social interaction (Cnaan and Parsloe 1989; Committee to Study the Impact of Info, National Research Council Commission of the U. S. 1994).

Simultaneously, due to the accelerated accumulation of information, the management of information poses a great challenge to the public and private sectors (Daler 1989, p. 13). Both internal and external threats may cause unexpected loss to individuals or organizations. The resources invested on information management have to be increased. In turn, information systems will further propel the advancement of the society.

Information and the legal gap

Digital information is a novel product of technological progress aimed at promoting social welfare through improving productivity. Information and other products of information technology, however, do not always play a positive role as people sometimes expect. In fact, many human expectations are left vacant in social reality. Society never previously got rid of unforeseeable trouble for information of a positive value and that of a negative value was not easily distinguishable or filterable before information systems came into being. Nowadays, both the information itself and the relevant technology have significance within the legal framework, because they should be either protected or prevented by law. Legal activities can involve information and ICT in different ways. The conventional legal notion is to be innovated to accommodate the inevitable role of information. The existing legal coverage should be extended to facilitate the protection or prevention of information processing and information abuse. Furthermore, co-operative preparedness and

jurisdictional adequacy are required for promoting the effectiveness of law enforcement.

Information and communications technology takes the traditional society into a brand new stage that people call the information age. The existence and development of the information society requires a feasible social environment. The primary tasks that the legal framework bears are to provide legal assurance for the healthy and orderly development of information and telecommunications, and electronic and mobile commerce. Law does so through facilitating growth and eliminating obstacles. The information society is accompanied by various concerns about data security and privacy protection. The prevalence of insecurity and infringement threatens the whole environment of the new technology, new economics and new welfare. Such insecurity and infringement lead to the creation of defensive and remedial legal instruments against cybercrime, composed of both substantive and procedural provisions, and of both domestic and international legal adequacy. The complete legal structure of the information society can be illustrated as the following:

Table 2 Facilitative Law, Protective Law and Remedial Law

Categories	Facilitative Law	Protective Law	Remedial Law
Functions	Facilitating growth, eliminating obstacles	Avoiding insecurity, preventing infringement	Domestic criminalization, and international harmonization
Coordinated sectors	International forum, Domestic forum	Public sector, private sector	Public sector, private sector

The topic of this dissertation contains no more space for facilitative law. The following sections are devoted to analysing the legal gaps accompanied by the proliferation of information systems.

The hysteresis of a legal notion

Many scholars regard information as the third form of protective object in criminal law, alongside person and property. Accordingly, the criminal-law theory has been adjusted to contain the new protective object. Some others, however, insist that

information is not the third protective object in criminal law; rather, they consider it as belonging to the category of property (Many of such arguments and discussion can be found in articles published in the 1980s, for example, BloomBecker 1981, pp. 16-17). They have criticized both the claim that information is the third protective object and the claim that information is not a protective object covered by criminal law.

Conventionally, "information" in the form of digits was not previously covered and thus not protected explicitly by criminal law. Just as traditional economic doctrines maintained that only land and manufacturing rather than the service sector produced real wealth (Stonier 1983, p. 25), traditional legal theories maintained that only wealth represented or produced by land and manufacturing deserved legal protection. However, once the requirement to protect information emerges, conventional concept has to meet the needs of social development. Therefore, to say that information was not and should not be protected by criminal law is outdated. In fact, the majority of scholars and legislatures have not accepted that it should be protected.

Information has been protected by criminal law in two ways. While there are people suggesting that law should not protect information, some others assert that information can be protected by a means equivalent to the protection of property. That is to say, information should be categorized as being in the same domain as property. People consider expanding the arm of criminal law to information just as they did to electricity.

On the other hand, from ancient to modern times, criminal law has in effect been handling crimes related to information in different forms other than the electronic one, such as libel, perjury, forgery, blasphemy, hate speech, copyright, trademark, patent, and so forth. In practice, information does broadly cover those specific traditional forms, such as oral, written, and printed forms, and more recently the forms stored, and transmitted by electronic, magnetic, and optical carriers, including the telephone, facsimile, radio, television, satellite, and nowadays computers and networks. When people face digitally computerized information, they pay a lot of attention to the existence of information in traditional forms, and thus give new life to traditional information crimes. Our general notion should be changed in order to adjust to the new ways of "thinking, writing, arguing, and valuing" in the information society (Lanham 1993, p. 229). The semantic practices of the latter society are to label everything with a mark of "information" or to refer to its physical vessel "the

computer" or to "the network."

It is an issue of "concept innovation" rather than criminal-law reform to recognize this point, but this concept innovation is necessary during criminal-law reform. Many crimes can be reconsidered in the light of the prevalence of the concept of information. With electronization, computerization, digitalization, automatization, and cyberization, these crimes become more apparently characterized as involving information. This justifies a wide expansion of punishment for the traditional offences involving information or information systems. Anyway, criminal law cannot demand a further expansion except through our understanding of the nature of these crimes. The social and technological developments have been impacting on criminal law.

The legislative gap

Information is an emerging object protected by laws designed to maintain social order and protecting social benefits. The conventional penal code has been designed to address crimes involving "tangible and visible objects" (UNCJIN 1999, Paragraph 84). The increasingly higher value of information poses unprecedented legal challenges, demanding new legal responses (ibid). Information has a value for specific owners and users. Cybercrimes often involve the illegal obtaining or destruction of information. Because information, programmes, databases, computer services or computer time, are intangible and invisible, conventionally the law has not recognized what to do regarding them and has difficulty in providing even the definitions essential to defend this type of property involved (BloomBecker 1983, p. 11). Because of the lack of a clear definition of information as a valuable interest, the existing law does not easily conduce to successful prosecution. What is needed is that the existing laws should be adjusted to guard the abstract "information" itself rather than merely the computers in which the information is generated, the media in which the information resides, the cables by which the information is transmitted, or the Central Processing Units (CPUs) where the information is processed.

The sphere to be covered by the new laws includes the use of ICT to make existing crimes more perceptible, to enable the inclusion of new forms of existing crimes, and crimes that specifically attack information systems (European Information Society Group, EURIM 2002). Some countries have taken action to

protect information as property in the traditional sense. On the other hand, some other countries exclude the concept of information from traditional crimes. Consequently, a noteworthy doctrine in criminal law rejects the independent position of information as one of the protective objects, which were conventionally confined to human being and property.

On the issue of information as property, there have been endeavours to adopt burglary law to acts of illegal access in which the cyberspace is supposed to be the equivalent of a domicile in genuine physical space. Nevertheless, in this endeavour, people ignore the distinction between the threats of the two offences. What is endangered in burglary is not what is endangered in illegal access. In burglary, what is directly endangered is the security of life and property. In illegal access, what directly endangered is the security of information. Information is not the equivalent of life and property, though it is likely to be indirectly pertinent to life, and can generate benefits or cause losses, or measured by a definite amount of money. The offences of illegal access, nonetheless, belong to the activities infringing the security of information, but not the right or security of life or property.

By using the terms traditionally used to indicate the misconduct in traditional offences, the offences against information seem to bear a similarity to traditional offences. Yet many people still doubt how a pair of hands can hold a piece of digital information. Strangely, we can frequently take notice of a question as "Can information practically be stolen?" The genuine uncertainty behind this question is "does information really exist in material form?" In addition, the intrinsic meaning potentially ignores the entity of digital information before human organs can perceive it. They accept only information printed on paper, shown on a screen, spoken in a backroom, transferred into a smell, or into an impression in any other form. Nevertheless, it is significant to note that the fact of obtaining information includes a pure perception of the content of the material. It is not necessary for the information to be physically moved or copied. For instance, the U. S. law criminalizes access to a computer without sufficient authority and thereby getting financial information, or to any information controlled by the government, and access to any confidential information where interstate or overseas business is involved in the criminal act (18 U.S.C. § 1030 (a) (2)). In many countries, the law further details the act of "obtaining data" by different terms, such as copy, output, and theft.

Digital information is not comparable to traditional property, and thus specific

legal provision is required to protect it. However, it is undeniable that information is often related to property, or even health and life. The protection of information will surely facilitate the protection of property, health and life. In different countries, punishments for offences against property and person involving information have different starting-points. Some countries directly apply traditional law to these offences, such as the Penal Law of China (See Articles 285-287 of Penal Law of China, 1997). The Articles 285 and 286 create several new offences in respect of information or information systems. And another article, Article 287, provides for the application of separate provisions in the Penal Law to penalize traditional offences, such as financial fraud, theft, embezzlement, misappropriation of public funds and theft of state secrets, and would now cover computer information systems, other than in respect of illegal intrusion and destruction. The Article indicates that all the offences that can possibly involve computer information systems are to be punished. Some other countries merely apply the law to acts involving information, as the law in the U. S. (See 18 U.S.C. § 1030). The 18 U.S.C. § 1030 creates several new offences targeted at information and information systems, and expands several traditional offences to acts involving information and information systems. However, the default doctrine is that the offences which possibly involve information and information systems, but are not criminalized explicitly by law, would not be punished.

Nevertheless, criminal law is also confronted with some other gaps brought by the rise of computerized information, specifically, the sphere of illegal access to and illegal interference with information and information systems. The Internet has a universal impact on the ways by which people acquire and transfer information. The opportunities for cybercrime are correspondingly increasing with the extensive access to computers and the Internet. To protect against cybercrime, effective actions at the local, national, and global levels can be taken (Sofaer and co-workers 2000). Nevertheless, the overall contemporary legislative situation is unsatisfactory: not all jurisdictions are covered by laws criminalizing cybercrimes; not all legislatures are synchronous with the development of technology and the abuse of it (Gelbstein and Kamal 2002, p. 3); and nor can people update their conventional notions all the time.

The jurisdictional discrepancy

The challenge to the contemporary legal system of digitalized information and its pertinent technology requires that countries with no law regulating the new object

should enact laws, and that countries with such law should harmonize their laws. The starting-point of this harmonization and cooperation is the creation of coordinated definitions of information and information systems. Some countries provide definitions of information and information systems in their criminal laws, but there exist substantial differences, though in the primary aspects they are comparable. In addition, the disagreement between the existing laws of different jurisdictions produces a safe haven for the perpetrators of many kinds of offences involving information and information systems.

Conclusion

Being informed is not necessarily beneficial. Informed by useful information, people can better compete in the social life. Informed by useless information, nothing better or worse will happen than a waste of time. Informed by harmful information, people would possibly weaken their own competitive force. Presently, all kinds of information are transmitted through the same information systems. Interference with transmission of useful information causes people to be less informed. Interference with transmission of harmful information –and even useless information- also causes waste in identifying the value of information. Cybercrime can lead to both of these situations. With the introduction of information and information systems into society, protection and prevention become the imperative tasks that jurisprudence, legislation, and law enforcement are confronted with. There has not been adequate preparedness to respond to cybercrime. The process of recognition and acceptance requires much time. The imperative requirement is for people to be well informed about the loopholes the legal system has and how they can be altered.

After clarifying in this chapter the potential change information systems can take to the legal system, particularly towards criminal law, the dissertation will begin to deal in the next chapter with the new criminal phenomena on the information networks, starting from a discussion about the exposure of the vulnerabilities of the networks to potential criminal activities.

References

Bjørn-Anderson, N. and co-workers. (eds) 1982. *Information Society*, North-Holland Press.

BloomBecker, Jay. 1983. Conscience in Computer: A Law Day Perspective on Computer Crime, *Computers and Society*, Volume13, Number 3, pp. 9-13.

BloomBecker, Jay. 1981. Employee Computer Abuse –What to Do? *The Los Angeles Daily Journal*, 3 August, pp. 16-17.

Cnaan, Ram A., and Parsloe, Phyllida. 1989. *Impact of Information technology on Social Work Practice*, Binghamion, New York: The Haworth Press.

Daintith, J. (eds.) 2004. *Oxford Dictionary of Computing*, fifth edition, Oxford: Oxford University Press.

Daler, T. Gulbrandsen, R. Melgrd, B. and Sjølstad, T. 1989. *Security of Information and Data*, Chichester: Ellis Horwood

European Information Society Group (EURIM). 2002. *Briefing No 34: E-crime – A New Opportunity for Partnership*.

Fisher, R. P. 1984. *Information System Security*, Prentice-Hall.

Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research, 2nd edition.

Heracleitus. 1979. *The Art and Thought of Heracleitus: An Edition of the Fragments with Translation and Commentary*, Cambridge: Cambridge University Press.

Johnson, L. R. 1970. *System Structure in Data, Programs, and Computer*, Prentice-Hall.

Konig, E. C. and Davidson, C. H. 1967. *Computers: Introduction to Computer and Applied Computing Concepts*, Wiley.

Lanham, R. A. 1993. *The Electronic Word: Democracy, Technology, and the Arts*, Chicago: University of Chicago Press.

Molitor, G. T. T. 1982. The Information Society: The Path to Post-Industrial Growth, in Cornish, E. (ed.), *Communications*

Tomorrow—The Coming of the Information Society, World Future Society, pp. 43-49.

Porter, Alan and Read, William H. 1998. *The Information Revolution: Current and Future Consequences*, Ablex Publishing Corporation.

Rabin, Jack and Jackowski, E. 1988. *Handbook of Information Resource Management*, New York, New York: Marcel Dekker.

Sofaer, A. D. and co-workers. 2000. A Proposal for an International Convention on Cyber Crime and Terrorism, Centre for International Security and Cooperation.

Sterling, Bruce. 1994. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Austin, Texas: Electronic Release.

Stonier, Tom. 1983. *The Wealth of Information: A Profile of the Post-industrial Economy*, London: Methuen London.

Tapscott, Don, Ticoll, David and Lowy, Alex. 2000. *Digital capital: Harnessing the Power of Business Webs*, Boston, Massachusetts: Harvard Business School Press.

United Nations Crime and Justice Information Network (UNCJIN). 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, Numbers 43 and 44.

Chapter IV Mixed Provision of Cybersecurity

Abstract

Based on the relative concept of cybersecurity, this article analyses the economic impact of cybersecurity breaches, identifies cybersecurity as a private good, and claims to implement the approach of mixed provision. The security protection should be principally borne by the private sectors, but the government is able to play an important role in establishing and enforcing the liability mechanisms. The mixed provision indicates that the close cooperation between the public and private sectors in security protection.

Keywords: cybersecurity, relativity, private good, mixed provision

Definition of cybersecurity

The literal meaning of cybersecurity denotes the security of information systems within the network environment. The security of information systems ranges over physical security of buildings, fire protection, software and hardware, personnel policies, and financial audit and control (Wood 1982, p. 9). In this dissertation, the primary concern is placed on the provision of cybersecurity and the necessity of public-private sectors.

In last article, we established the classification method according to value of information. Although the value of information differs from each other, cybersecurity is a value-neutral conception. There is no distinction between virtue and vice other than the limit of security and insecurity. Nevertheless, the security of information systems is presumably pertinent to the security of information with positive value. Since the value judgment is not a technical but a legal problem, the technical conception of cybersecurity necessarily affects the legal conception. Consequently, the legal conception of cybersecurity does not always consider the problem of virtue and vice. Either the legislature believes that the virtue and vice of information is not judged by individuals, or even if the legislature considers the information vice, it cannot be punished by individuals. Therefore, literally, cybersecurity covers the

protection of information with different values without distinction between virtue and vice. It is possible to say that law goes to the corner in the problem of cybersecurity.

Security is freedom from risk, danger, or crime. Cybersecurity protects "information systems against unauthorised access to or destruction, alteration and modification of information, whether in storage, processing or transit, and against the denial of service to authorised users, including those measures necessary to detect, document, and counter such threats" (National Security Telecommunications and Information Systems Security Committee (NSTISSC) 2003, 33). The importance of information systems in the individual life, institutional operation and governmental administration determines the same importance of cybersecurity. The breach of security could bring about domino effect in the chain of information processing. Immense impairment can be caused not only by an act, but also by the panic, the loss of confidence, the injection of doubts and hesitations, and the destruction of trust (Gelbstein and Kamal 2002, p. 1). Nonetheless, perfect security does not exist (Howerton 1985, p. 55). The maintenance of a higher degree of security rather than perfect security becomes a goal that the users of information systems are chasing.

Cybersecurity comprises of physical security and spiritual security. On the one hand, cybersecurity is generally comprehended as technical guarantee, varying from peripheral surveillance, lockup of hardware, user name and passwords assignment, anti-virus software, to installation of firewall. The typical computer security measures in the computer rooms of a Finnish university, for instance, include all of the above respects. The surveillance system is installed inside the gates of the buildings to monitor the exits of the premises. Computers are safeguarded with metal boxes, chains, and locks to prevent from theft. The access control is realised by assignment of user names and passwords to authorised users. "F-secure" is installed in every computer, with the functions of anti-virus, firewall, etc. Technical guarantee is the kernel of the cybersecurity in the physical layer. On the other hand, due to the insufficiency of technical measures and threats from cybercrime, legal actions act as the kernel of the cybersecurity in the spiritual layer, which consists of regularisation of the authorised access and penalisation of the unauthorised access.

If information systems are insecure, malicious individuals have an incentive to spend resources trying to acquire unauthorised access, while the owners or users have an incentive to spend resources keeping information systems from being compromised. However, the conception of security has always hanged behind the

philosophy of innovation towards convenience and efficiency. As the Cornell Commission pointed out that, “[a] community of scholars should not have to build walls as high as the sky to protect the reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information” (Eisenberg et al. 1989, p. 707). That is true regardless of whether the unauthorized access is private or public. Therefore, insecurity of information systems creates negative externalities, as it potentially accommodates the computer worms, distributed denial of service and so on.

Compared with investment on information systems, the investment on cybersecurity is a pure social cost. The loss induced by cyber insecurity is also a pure social cost. The cyber insecurity can have great side effects. First, insecurity causes the wave of employment of the personnel involved in cybersecurity: security software developer, cyber police, and the recruitment of prosecutors, judges, and prison managers. Second, insecurity becomes the reason of redistribution of wealth: the incidences of cybersecurity breaches are the best excuse for imposition of taxes by the government, and the enlargement of judicial system. Third, insecurity becomes the route of redistribution of wealth: the wealth is redistributed from the users to the judicial system, through the threats caused by the intermediary of the attackers.

Therefore, the cybersecurity institutions in the electronic market are acquainted well with what their best way to benefit from the social requirements. The moral hazard would not prevent them from being thrilled to see increasing incidences of cybersecurity breaches.

The long established theoretical foundation has discussed information security in three aspects, that is, confidentiality, integrity, and availability (For example, Parker 1981; Wood 1982, p. 4; Bishop 2003, pp. 3-6). Confidentiality is the concealment of information or resources, protecting from unauthorised disclosure to individuals, processes, or devices (Fischer-Hübner and Swimmer 1993, p. 92. See also National Security Telecommunications and Information Systems Security Committee (NSTISSC) 2003, p. 17). In fact, any security protection software and hardware are prone to deliberate breakdown. As a result, however complicated they are created, however frequently they are updated, and however many potential security flaws they fix, the attack technique will pace with it in a short time. Even at present, confidentiality is still supported by access control mechanism, which is usually realised by cryptography, scrambling data to make it incomprehensible.

Integrity refers to the trustworthiness of data or resources (Mulholland 2004, pp. 7-8). It guarantees that data contains the correct physical and semantic representation of information (Fischer-Hübner and Swimmer 1993, p. 92). The value of information requires the information to be retrievable as a whole. Incomplete information can result in either unavailability or misleading effect.

Availability refers to the ability of timely, reliable access to data and information services for authorised uses (National Security Telecommunications and Information Systems Security Committee (NSTISSC) 2003, p. 7). Availability is often the most important factor in service-oriented businesses (General Centre for Internet Services 2003). The unavailability usually indicates the interruption of the business and direct loss from transaction and indirect loss of reputation. Maintaining availability requires the stable information systems and the harmony of peripheral environment.

Besides the above three aspects, Mulholland (2004) also mentioned authorisation, authenticity and non-repudiation at the same time. On all accounts, information security is the security despite of the value. Virtue and vice are both protected comparably. If the information is secured firmly, information with positive value and its transmission avoids unauthorised access, while information with negative value and its transmission also evades the legal interception and surveillance. By contraries, if the information is vulnerable, information with positive value and its transmission is prone to be accessed without authority, while the disclosure of crimes related to information with negative value and block of its transmission becomes easier. The functional areas of information security include risk avoidance, deterrence, prevention, detection, and recovery. It is also frequently defined in terms of several interdependent domains: physical security, operational and procedural security, personnel security, system security, and network security (Ross 1999).

Relativity of cybersecurity

There are various answers to the question of "What is cybersecurity?" Cybersecurity is a comparative concept. On one hand, it comprises the comparison between security technique and the attack technique. On the other hand, it comprises the comparison between different security techniques and measures. In the aspect of

comparison between the security technique and attack technique, it is well publicly recognised that the attack technique develops faster than security technique, regardless of what are the exact reasons. Take it the other way, the hardware, software, or any other components of information systems are always vulnerable and can be exploited. We could consider this imperfect security as the absolute level of security. In the aspect of comparison between the different security techniques, the existence in the different environment, the possession of different hardware, software and other equipments, and the adoption of different techniques all cause the difference of the security levels. Therefore, each of the individual and organisational users maintains a specific level of security.

Some viewpoints regarded the cybersecurity as an externality. Camp and Wolfram (2000) pointed out that if a company does a poor job at cybersecurity, other companies might be affected negatively. Accordingly, the cost is an externality to the owner of the infected machine (Camp and Wolfram 2000). Nonetheless, if we identify cybersecurity as an externality, it is inevitable that to the extent investments in cybersecurity create positive externalities, too little will be provided.

Security is not the reason that causes the attackers to violate the security and launch the attacks, nor the condition that facilitates the attacks, but the target that the attacks aim at. In fact, there is no clear limit between security and insecurity. Security and in security have only quantity difference, but no quality distinction. Neither absolute security nor complete insecurity exists. That is to say, security and insecurity should be security between zero percent and 100 percent. Therefore, security is a relative concept. The security of a higher degree is security, while the security of a lower degree is insecurity.

Although information systems on the Internet all have the similar framework, they lack any central controlling system, and are uncontrollable. Not only the physical system but also the operation process is uncontrollable. Therefore, to a great extent, the security of information systems depends on the security measures by the end users, either individuals or organisations. However, the security measures of individual and organisational users are extensively dissimilar due to the difference of their hardware, software, and human resources.

The degrees of security of the end users on the network are different, there does not exist an absolute value of security. Security is exactly a compare of relative value. It is both the result of compare between users, and the compare between the past and

the present, i.e., the horizontal compare and longitudinal compare. Because of the vast number of the network users, and the rapid change of the network environment, the result of the compare change constantly. In general, the security of a higher degree will change fast into the security of a lower degree (insecurity) with the transformation of technique and environment. Therefore, the cybersecurity measures must be updated and renewed timely, frequently, and efficiently.

If the cybersecurity measures cannot be updated and renewed timely, frequently and efficiently, the vulnerability might emerge. Vulnerability is not security or insecurity, but a factor that makes it impossible to realise perfect security, and an extra discount caused by the external factors in the investor's production of the expected complete security. It is the natural adversary of the security product, i.e., loopholes that can be detected and exploited by the potential attackers to commit harm and cause loss. As Denning and Denning (1979) remarked on the data security, that even all the technological internal security controls of any kinds can only reduce the risk of compromise to an acceptable level, but are subject to limitations in achieving their objectives under all conditions (Denning and Denning 1979, pp. 227-249).

Economic impact of cybersecurity breaches

Cybersecurity breaches have multi-dimensional economic impact on states, users, and particularly, the victims.

Firstly, as an integral part of the homeland security, cybersecurity costs countries' budget in a rising rapidity. Relatively an undersized proportion within the entire budget, these expenses will inevitably bring about new financial burden to the taxpayers of the whole country.

Secondly, the users' investment on cybersecurity takes on the tendency of increasing. According to the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) (2005), nearly all of the companies surveyed in 2005 used anti-virus software, firewalls, and some measure of access control. These measures induce the increase of the investment of network users. However, in fact, security measures can never be a perfect assurance against damage and accidents.

Thirdly, although the investment is increasing, the cybersecurity breaches occur frequently. The potential for information security breaches, as well as the magnitude

of potential losses associated with such breaches, has been confirmed by empirical studies.

The annual surveys on information security breaches have pointed out that cybersecurity breaches are ubiquitous. The 2005 survey conducted by CSI and FBI noted that 56 percent of the 693 United States computer security practitioners acknowledged the unauthorised use of a computer in their organisation in the last 12 months. Given the proprietary nature of this issue, it is reasonable to assume that information security breaches are far more common than indicated in the various studies addressing this issue.

Fourthly, as a consequence of the frequent occurrence of cybersecurity breaches, the losses of these breaches are increasing. The cost of a cybersecurity breach can be measured by both “tangibles” and “intangibles” (D’Amico 2000, p. 1). In Forrester Research, Howe et al (1998) estimated the tangible and intangible costs of computer security breaches in three hypothetical situations. Their analysis indicated that, if thieves were to illegally wire one million dollars from an online bank, the cost impact to the bank would be 106 million dollars.

The 2005 CSI and FBI survey noted that, of the 639 respondents that were willing and/or able to estimate losses due to security breaches, such breaches resulted in losses close to 130 million dollars. In comparison to the dollar value of losses associated with information security breaches not acknowledged, this figure probably pales. Furthermore, even in organisations that are willing to acknowledge the dollar value of losses associated with information security breaches, accurately deriving the accurate figure is problematic, including the difficulty in deriving the dollar value of lost sales due to the negative “reputation effect” of a publicly known security breach.

Provision of cybersecurity as a private good

Assumed a public good, cybersecurity would be underprovided or fail to be provided at all in the private market. Nonetheless, since individuals are not generally liable for the damage caused when a hacker takes over their computer, they do not benefit from the increased security (Varian 2002). Since the user with the ability to provide the security does not benefit, they will fail to provide it.

Traditionally, defence is regarded as a pure public good, observed from the standpoint of domestic individuals and organisations. If observed in the entire world,

the various states' national defence is essentially private goods. Various countries' national defence is purely for self-interest, but not altruistic. The strengthening of national defence by each state is as the similar as a household lock its own gate. According to the traditional economic analysis of law, this seems to violate the reciprocity of neighbourhood. State A as a potential aggressor purports to commit aggression against another states B or C. Because state B has the formidable national defence, for instance it has the nuclear weapons, then state A will turn to attack state C, which has weak defence. Thus according to the traditional analysis, for both state B and state C to create formidable defence, it will be inefficiently excessively invested. Therefore, state B and state C should form super-national coalition to provide common defence system. Under such circumstances, both state B and state C are required to undertake the expenses involved in the production of the national defence by the super-national institution. The expense might not only equal to the summation of the previous defence expenses of the two countries, but might be higher than this sum, due to more transaction costs. Moreover, it can also cause the free-rider’s problem. For instance, state C might free-ride. State B might invest massive funds, while state C does not provide any help. The state B is naturally dissatisfied and therefore unwilling to pay any more. Therefore, state B might also free-ride on the super-national institution’s operating. At last, the super-national institution becomes ineffective. Both state B and state C become free riders. What is worse, if there were other countries, all of them would do so as well. Therefore, the super-national institution cannot play any role in national defence. All of the state B, state C, and states D, E, F…know exactly how other parties are thinking about and what the other parties are doing (free-riding), while the super-national institution could not function at all, then, all of them would not trust the super-national institution any more. The end returns to the commencement, and each state produces its own defence. Consequently, at the international level, defence is a private good of each country.

From Kobayashi’s (2005) viewpoint, cybersecurity is not analogous to the traditional security. To discourage crime e*x ante* in the general criminal context, the government can implement the sufficient level of punishment to deter the crime from accruing. In the case of cybercrime, the likelihood of detecting is so low that the penalty inflicted would have to be of enormous magnitude to discourage cybercrime.

It is important to distinguish computer security from national security (that is to

say, distinguishing externalities from public goods) because the solutions to public goods problem and to externalities differ.

As we have seen that, cybersecurity has both exclusiveness and rivalrousness. Cybersecurity has neither territorial boundary nor industrious limit. In the global village, all individuals and organisations are confronted with risks of the equivalent level. Under this environment, the security of individuals or organisations' systems matter firstly themselves. Only in accidental situation are others involved in, such as in the case of distributed denial of service attacks.

Powell (2005) provided evidence from the financial services industry to prove that the cybersecurity is hardly a public good. We can understand that individuals and organisations have the exclusiveness in the cybersecurity. The exclusiveness of cybersecurity roots in the three characteristics of cybersecurity, specifically, confidentiality, integrity and availability, among which confidentiality fully expresses the exclusiveness of cybersecurity. If the security is available to one user, it is unavailable to other users. If others enjoy the security, the user's security cannot be maintained any longer. Unsurprisingly, cybersecurity is characterised as the preservation of confidentiality, ensuring that information is accessible only to those authorised to have access; integrity, safeguarding the accuracy and completeness of information and processing methods; availability, ensuring that authorised users have access to information and associated assets when required. The security of information systems is enjoyed solely by users themselves. Any share by others, their systems become insecure. In fact, hackers are precisely the exploiters and sharers of the insecure systems. Therefore, cybersecurity has more exclusiveness than any private goods.

On the other hand, the cost of expanding security to others is not zero, but enormously expensive. If one user enjoys a higher degree of security, the degree of the others' security will relatively decrease. As mentioned above, there is not perfect security. Security and insecurity are relative concepts, which exist in the comparison. If one enjoys a higher degree of cybersecurity, the others' security degree will decrease to insecurity. The competition in the security measures is the reason that causes the increase of the difference between the relative securities. Of course, the competition benefits to the enhancement of the total security level.

Some study (such as Katyal, 2006) insisted that to some extent private security measures might increase crime. The basic assumption of this argument is that, if one

household lock its door, the thief will turn to the neighbourhood whose doors are left unlocked. Therefore, locking of one's own door is breaks the reciprocity and mutual trust among the neighbourhoods. If we consider the fact that presently almost all households, companies, and even government agencies lock their own doors, we can uncover without difficulty that the assumption is excessively implausible. Only when every household, companies, and governmental agencies are convinced not to take such "inefficient" measures is such an assumption significative. Such an assumption ignores the dual values of locking in the prevention of crimes. On the one hand, locking protects oneself from damage and harm, making the potential criminals shrink back at the sight, or costing criminals more time before suffering losses. On the other hand, locking increases the potential criminals' time consumption and material costs in looking for new victims, and even making it impossible for them to find one. If none of the households and organisations locks their doors, potential criminals can easily find possible targets. Therefore, the difficulty of crime will decrease, and the efficiency will increase. The potential criminals are indifferent in case the costs, benefits, likelihood of success.

Cybersecurity is particularly in such a situation. If every computer is encouraged not to use security control, they will be more vulnerable in front of the attacks. Assuming that the capability and environment of all the individuals and organisations' computers are the equivalent, and the risks of being attacked also roughly the equivalent, then only when their benefits related to the cybersecurity are also the similar could the provision of public cybersecurity efficient. Nevertheless, this situation seldom exists in reality. Therefore, a delimited public cybersecurity would be superfluous for some individuals and organisations, and be insufficient for others. For the situation of superfluousness, it is economically inefficient; while for the situation of inefficiency, it is ineffective in security. Therefore, both ways, the public cybersecurity control cannot function optimally. Hence, if cybersecurity is provided with the mode of public good, it is impossible to be more beneficial than as private good.

Now that cybersecurity is a private good, can individual and organisational users afford for the production and provision of the security? Katyal (2006) argued that if governments do not act to deter cybercrime, only wealthy companies could afford for the security measures to protect themselves. At the same time, if the governments tell companies that they will not punish the crimes, the companies will not use the

networks any more, hence the utility is reduced. Nevertheless, greater security measures are possible to cause distributional concerns. The activity of the governments punishing the cybercrimes is essential, including legislation and justice. Only when the governments continue to punish cybercrimes do they treat the individuals and organisations equally in playing their role. It is necessary to note that the role of governments in the cybersecurity is not direct maintainer, but indirect deterrent of cybercrimes.

Unlike national defence that unless it is produced as a pure public good, individuals, and organisations are unable to undertake the responsibility. Nevertheless, other public goods are more or less of the properties of private goods, if they provided as pure public goods, it would be inefficient and ineffective.

On the other hand, when we inspect the provision of cybersecurity by the government, the questions exist in the provision of public goods are the efficiency of the government and the tax burden of individuals and organisations. On the one hand, regarding the efficiency of the governments in maintaining the cybersecurity, they are not particularly good at providing technical measures for ex ante cybersecurity. Indeed, individual companies produce most of the current cybersecurity software and hardware. If the governments use these companies' products to maintain the cybersecurity, they are only the users but not the producers of these products. This fact does matter in that the government uses the products, to which they contribute nothing more, to maintain the cybersecurity, and in the end impose on the individuals and organisations that pay the bill. They are as the equivalent as intermediaries, who bring about further transaction cost but no substantive change in effect

The incentive of individuals and organisations to pay tax would be absent, because of the fully awareness of the impossibility of undertaking the responsibility of providing cybersecurity by the government, while the individual measures of cybersecurity are inevitable. Such taxation arrangements, lack of support from the public opinion, are difficult to stand. Therefore, the public cybersecurity safeguard will break down eventually. On the other hand, the renewing of the products of cybersecurity is more rapid than the traditional security products. The individuals and organisations' systems and situations differ in thousands ways that the government could hardly catch up with the steps upgrading. Therefore, the taxation would not be efficient.

The frequent occurrence of the security breaches and the huge loss of the users

represent the scarcity of the cybersecurity. It can be well assumed that, the investment on cybersecurity does not improve the users' productivity. Given the security breaches always occur by a certain probability, which is less than 100 percent, from the viewpoint of market competitive, the costs can never be imputed from some users to others. Once a user investment on cybersecurity, he loses completely the sum of the investment. If he or she does not investment on the cybersecurity, the sum of the investment is saved, and the possible loss only exists with some probability. Here, the risk exists in both the occurrence of the security breaches, when the users endure an expected loss of a certain probability; and the non-occurrence of the security breaches, when the users endure a pure loss of the entire sum of the investment. Therefore, it is not easy for either risk averter or risk lover to decide to invest on cybersecurity after considering such risks. When the user makes zero dollar of investment on cybersecurity, it is possible to say that he values the expected benefit from the security as zero, too. Although the probability of security breach is high and the security level is low, the system is more vulnerable to outside attacks, and his expect loss in security incidence is larger, he is indifference to it. This equals to that he is indifference to his benefit related to the network, intentionally or unintentionally.

If the hacker values the security violation as high as 1,000 dollars, and he obtains unauthorized access to the system with great satisfaction. The consumer's surplus of the hacker equals 1,000 dollars. He must pay the price to society through the criminal sanction or to the victim through civil remedy. Because the probability of detection of his hacking is low, the criminal sanction or the civil remedy should be severe enough play a role of deterrent. If the probability of the trans-national detection is zero percent, hackers in the "haven" countries are always determined to hack into systems located in other countries, without the risk of being arrested and the possibility of pay for the game.

There would be potential hackers who value the security more than the users, and who are willing to pay more than the users, by means of fine or imprisonment in cases of criminal sanctions or damages in cases civil remedy. If some users are willing to subject their benefits related to the network to the potential hackers, the market will be operated so that the consumers' surplus is higher on the part of the hackers.

Mixed provision of cybersecurity: cooperative and liability mechanisms

Even if it were technically feasible to keep all systems absolute secure, the costs would be so prohibitive as to render such an approach an economic prescription for catastrophe. The government can neither provide cybersecurity nor manipulate the systems. Naturally, one of the Ernest and Young survey's (2004) key findings was that only 11 percent deemed government security-driven regulations as being highly effective in improving their information security posture or in reducing data protection risks. Nonetheless, any argument thinking that the governments can play no role in the field of cybersecurity is over sceptical. The governments can play a necessary role in deterring the attackers, but they are by no means helpless in the maintenance of the cybersecurity. Their roles are to impose penalty through legislation, and deter crime by means of ex post law enforcement. Providing cybersecurity as a public good is confronted with greater difficulties in international cooperation than as a private good. Even if some countries can convince their taxpayers to pay for the expenses involved in the public provision of the cybersecurity, if you cannot simultaneously convince all countries to do so, it will not cost-efficient. The further analysis included in this dissertation will provide more evidences for this argument.

In the meanwhile, a consistent set of themes from individual, organisational, national, regional and international cybersecurity strategies are emerging, for example, as Sadowsky (2003) listed, the public-private partnership (The cooperation between private sectors and law enforcement in combating cybercrime has been widely accepted by scholars, for example, Levinson 2002, pp. 526-527); public awareness; best practices, guidelines and international standards, information sharing; training and education; respect for privacy; vulnerability assessment, warning and response, international cooperation, and so on (Sadowsky et al 2003, pp. 170-172). The projects fully coincide with the recognition of the nature of cybersecurity in this chapter.

Conclusion

Cybersecurity has the characteristics of a private good and seems feasible to be provided mainly by private sector. The public provision of cybersecurity would have the negative effect of discouraging the private sector to invest less in the security

protection. From this standpoint, if the government intervention is taken in early stages, the financial burden would be unnecessarily aggravated and practical effect would be naturally weakened. Nevertheless, at the aspect of prevention of various forms of serious security breaches, the law enforcement can play an important role in establishing and enforcing the liability mechanisms, where the private sector lacks of sufficient power to remedy deal with the breaches. Although it is still controversial on whether and how the cybersecurity players should be held liable for their own activities, every steps made towards this direction will benefit the private sector to achieve their goals. It has been widely acknowledged that the cybersecurity is field accommodates the development of public-private coordination.

Apparently, the mixed provision of cybersecurity could more easily be accepted due to its responsibility and liability distribution. Utterly private provision of cybersecurity is confronted with the liability evasion of the interest-driven strong groups, usually the giant service providers. They are generally willing to extend their security protection to the end users, but they are unwilling to leave any possibility to undertake any liability when there is security breach happening. It is so that if they leave a liability door open to one user, they must leave the door open to all the users. As a result, every Internet service provider has its strict disclaimers closing the liability door for all the users, so as to diminish its risk in vulnerable information systems. Definitely, this does not mean that these enterprises are blind to the threats against the security. In fact, many of the enterprises endeavour to update their security protection, in order to solicit more customers and to win the competition. It seems that it is only a problem of time for the private sector to provide the security more actively with a broader coverage. To some extent, this is also a requirement of the market mechanism, further proving that the private provision would be accordant to the nature of cybersecurity.

Subsequently, the public-private coordination in cybersecurity provision has the capacity to improve supplement with each other. The public sector is anticipated to have insufficient resources to fully provide cybersecurity, because the public provision will completely discourage the private investment. The private sector would on one hand have the incentive to evade liability if there is no liability mechanism outside the market, and also have the incentive to attract users who are seeking for more secure a system on the other. Lack of any one of the two sectors, cybersecurity might be confronted with problems that are more serious. Mixed

provision, that is to say, public-strengthened private protection has the unique advantage.

References

Bishop, M. A. 2003. *Computer Security: Art and Science*, Addison-Wesley Professional.

Camp, L. J. and Wolfram, C. 2000. Pricing Security, in *Proceedings of the CERT Information Survivability Workshop*, Boston, Massachusetts, 24-26 October, 31-39.

D'Amico, A. D. 2000. What Does a Computer Security Breach Really Cost? Retrieved 14 January 2009, from http://www.securedecisions.com/documents/CostsOfBreaches-SANSInstitute.doc

Denning, D. E. and Denning, P. J. 1979. Data Security, *Computer Surveys*, Volume 11, Number 3, 227-249.

Eisenberg, T. et al. 1989. The Cornell Commission: On Morris and the Worm, *Communications of the ACM*, Volume 32, Number 6, pp. 706-709.

Ernest and Young, 2004. Global Information Security Survey 2004, BYG No. FF0231, Retrieved 14 January 2009, from http://www.ey.com/global/download.nfs/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf

European Communities. 1991. *Information Technology Security Evaluation Criteria (ITSEC): Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom*, Printed and published by the Department of Trade and Industry, London.

Fischer-Hübner, S., and Swimmer, M. 1993. Social Aspects of Computer Virus, in Beadon, C. and Whitehouse, D. (eds.), *Computers and Society*, Oxford, London, pp. 91-107.

Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research, 2nd edition.

Howe, C. et al. 1998. *The Forrester Report: Economics of Security*, Forrester Research.

Howerton, P. W. 1985. *Computer Crime: A Tutorial*, ACM.

Katyal, N. L. 2006. The Dark Side of Private ordering: The Network/Community Harm of Crime, in Mark F. Grady and Francesco Parisi, eds, The Law and Economics of Cybersecurity, Cambridge, new York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo: Cambridge University Press, pp. 193-220.

Kobayashi, B. K. 2005. Private versus Social Incentives in Cybersecurity: Law and Economics, in Mark F. Grady and Francesco Parisi, eds, *The Law and Economics of Cybersecurity*, Cambridge, new York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo: Cambridge University Press, pp. 13-28.

Levinson, D. (ed.) 2002. *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.

Mulholland, J. 2004. *Florida Cybersecurity Manual*, Florida Department of Law Enforcement, Secure Florida, and Florida Cybersecurity Institute.

National Security Telecommunications and Information Systems Security Committee (NSTISSC). 2003. *National Information Assurance Glossary*, CNSS Instruction Number 4009.

Parker, D. B. 1981. *Computer Security Management*, Prentice-Hall.

Powell, B. 2005. Is Cybersecurity a Public Good? Evidence from the Financial Services Industry, *Independent Institute Working Paper*, Number 57.

Ross, S. T. 1999. UNIX System Security Tools, McGraw-Hill Osborne Media, 13 September. Retrieved 14 January 2009, from http://www.albion.com/security/intro-4.html

Varian, H. 2002. System Reliability and Free Riding, in *Proceedings of the First Workshop on Economics and Information Security*, 16-17 May, University of California, Berkeley.

Chapter V Extension of Victimization: Unsolicited E-mail Messages with Attachments

Abstract

While the growing scale of Internet use brings about great convenient for users, phenomena of unsolicited e-mail pose new threats and challenges. Previous literature was concentrated on general analysis of such messages, leaving many particular respects untouched. This study focuses on the extension of victimization of unsolicited messages e-mail with attachments (UEMAs). Based on the analysis of two samples, one comprised of 501 (sampling done in May 2006), and the other comprised of 490 (sampling done in March 2008),pieces of UEMAs, the study finds that e-mail account exposing and seeking can both contribute to victimization; while receiving of unsolicited messages is the initial victimization, reading and reacting to messages could lead to additional victimization from virus attack or financial fraud, and from conspiracy in illegitimate operations such as tax evasion or transaction of falsified documents.

Keywords: E-Commerce, Survey, Cybercrime, Unsolicited E-mail Messages with Attachments (UEMAs), Victimization, Conspiracy

Hacking all the way into spam

The twentieth century witnessed many outstanding creations of human beings, of which the Internet is one extending its power to today. Radical group (2005) found that more than 683 million users held 1.2 billion e-mail accounts in communication and marketing. It implied that, besides other things, each user could have more than one account. In practice, many frequent users have two or more accounts. Despite the convenience that this unprecedented tool creates, unsolicited e-mail message, its by-product, becomes a nuisance that each user meets by chance. Recipients' property

rights, fair trade, public morals, cybersecurity, data protection, as well as other content-related and goods-related transgresses and offences all pose great challenges and threats to society that is symbolized by cyberspace (Li 2006).

Many people have no interest in talking about this issue. Even some economists, whom I had conversation with in a conference in 2005, ignored the significance of such a research. Their straightforward logic was that "unsolicited e-mail is everyday phenomena; everyone knows something about it; and no one thinks it so serious." One of the economists told me that he received spams everyday and deleted them in a few seconds without extra trouble. They tended to devaluate the academic subject by ignoring the impact of the research object through raising examples in their own life, which seemed to be strong enough proof and sound enough understanding.

However, numerous authors have scrutinized the phenomenology of unsolicited commercial e-mail (UCE, or unsolicited business e-mail, UBE, or simply spam) from points of view of economics, commerce, law, technology, sociology, culture, and so on. Others have principally dealt with costs and benefits of senders and recipients derived from unsolicited e-mails (Khong 2001, and 2004), general impact on productivity of individual employees and enterprises (Nucleus 2003, 2004), scale and volume of unsolicited e-mails (Radical Group 2005), impact on consumers' attitudes and confidence towards e-commerce (TACD 2003; Fallows 2003; Harris Interactive 2003), higher possibility of receiving unsolicited e-mail due to online-published addresses (Federal Trade Commission 2002b), ignorance of removal requests by senders (Federal Trade Commission 2002a), and technical and legal solution on unsolicited e-mail (Sorkin 2001).

Few studies, nevertheless, have touched on unsolicited e-mail messages that have attachments, particularly on what kind of risks a single e-mail user might face. In this study, I use two samples, one comprised of 501 pieces (sampling done in May 2006), and the other comprised of 490 pieces (sampling done in March 2008), of unsolicited e-mail messages with attachment, presenting the first analysis of types and validity of sender column, types and validity of subject column, types of offers of message content, and types, sizes and nature of attachments of these messages. In this paper, the term "spam' is deliberately taking into account the lack of a universally-accepted unified definition. At the same time, the author prefers the phrase of "unsolicited e-mail" without the modifier "commercial" or "business", in order to enlarge the coverage of UEMAs to virus spreaders in this study.

Literature review

At the same time as the augmented capacity of computers and networks to process information, “a wealth of information” could results in a “poverty of attention” (Simon 1982). Unsolicited business e-mail (UBE) or unsolicited commercial e-mail (UCE) incarnates an instance where e-mail users have to deal with redundant information they anticipate not to consume. Unsolicited e-mail gives rise to an unconstructive representation of e-marketing, alarming e-mail users from trusting e-mail communication.

Unsolicited e-mail sent out to multiple recipients has extensive unfavourable consequences on e-mail marketing. Karnell (2002) found that an increasing number of e-mails had never been read by recipients, and users prefer limiting or disrupting business contacts with these senders. The prevailingness of unsolicited messages exhibited an emergent intimidation to the information society (World Summit on the Information Society 2003, paragraph 37).

Spammer-X (2004) narrated his/her anecdote with reference to reasons and methods of spamming, revealing the astuteness of defeating anti-spam techniques, avoiding being identified, in addition to escaping the law. McWilliams (2005) accounted the world of spammers and spam-fighters, furnishing information on mechanisms of spamming and spam-fighting. Goodman (2004) presented the most typical spam traps and explained why existing solutions were ineffective. Lambert (2003) analysed a wide range of e-mails in attempt to generate a silhouette of spam and develop a profile of spammer.

The United States Federal Trade Commission (1998) speculated the issue from the standpoint of consumer protection, identifying a dozen of most likely spam scams, covering spam and scams from business opportunities, quick money, working at home, to guaranteed loans, and so on.

My study (Li 2006) recapitulated six challenges that the spam brought to society: recipients’ property rights, fair trade, public morals, cybersecurity, data protection, as well as other content-related and goods-related transgresses and offences. From the standpoint of senders, all these challenges could be classified into two bigger categories: victim seeking and conspirator seeking. From the standpoint of recipients, they were confronted with preliminary victimization (being spammed),

supplementary victimization (being defrauded, or attacked by viruses), or committing offences (tax evasion, or transaction and use of falsified documents).

Nucleus (2003) reported in-depth interviews with 117 employees and extensive interviews with 28 IT administrators. They found that an average of 13.3 unsolicited messages reached the employee per day; each employee has to waste an average of 6.5 minutes per day dealing with unsolicited messages. They calculated that unsolicited messages caused an average 1.4 percent of productivity loss per employee per year, tantamount to an average cost of 874 dollars per employee per year.

Nucleus (2004) reported further interviews with employees at 82 Fortune 500 companies. They found that users received an average of twice the number of previous year's unsolicited messages, with an average 3.1 percent of productivity loss in 2004. They also established that the function of technical solution to unsolicited messages became less efficacious.

Fallows (2003) reported the Pew Internet & American Life Project, which collected data from a national telephone survey of 2,200 adults and a compilation of more than 4,000 first-person narratives about unsolicited messages. Their findings showed that unsolicited messages caused some e-mail users to use e-mail less, and trusted the online environment less, while fear of unsolicited messages increased.

The deteriorated consumers' confidence on unsolicited e-mails results from the losing control over their own accounts. Federal Trade Commission (2002a) tested 215 addresses from spam with "remove me" claims, and found that unsubscription demand was usually ignored. While senders of unsolicited e-mails do not provide effectual unsubscription method, they are harvesting addresses from all over the Internet.

Federal Trade Commission (2002b) put 250 new, undercovered e-mail addresses in 175 different locations on the Internet, including web pages, newsgroups, chat rooms, message boards, and online directions for web pages, instant message users, domain names, resumes, and dating services. They found that web pages, newsgroups, and chat rooms were all attractive to unsolicited message senders. Federal Trade Commission (2005) found that spammers continued to harvest email address posted on web sites, and to a much lesser extent, those posted on blogs and USENET groups. Masking email addresses when posting on web sites could substantially reduce the risk of harvesting.

Federal Trade Commission (2003a) reported that 66 percent of spam messages were fraudulent in sender or subject columns, or in the message itself. False advertisements might distort the normal market of goods and services, harm the normal trade order, and reduce the consumers' confidence (The Directorate General of Telecommunications Ministry of Transportation and Communications 2005, pp. 6-7). Large volume of spams, malicious programs and malicious linkages contained in messages were main threats (PC World 2003).

Harris Interactive surveyed 2,376 adults online in 2003, and found that most online adults reported that they had received more spam than six months earlier. Only 14 percent have seen a decline in the volume of spam. A majority of respondents reported unsolicited messages annoying or very annoying (Taylor 2003).

Many spammers send messages by unauthorized use of accounts of other individuals or organizations (Organization of Economic Cooperation and Development 2004). E-mail addresses harvesting software can collect this information automatically from web pages (Boldt, Carlsson and Jacobsson 2004, p. 8). Based on discussion of spyware and findings from two experiments, Boldt, Carlsson and Jacobsson (2004, p. 4) concluded that spyware had a negative effect on computer security and user privacy. Spyware enables spreading of e-mail addresses that may result in receiving unsolicited e-mails.

Khong (2004) stated that although it was difficult to measure costs and benefits of the spammer, if the benefit obtained from the activity outweighs the cost, the spammer would carry out spamming activity. It follows that if there is one successful commercial transaction, the spammer can realize his or her benefit. The costs that are involved in the spamming can be roughly estimated according to costs of bandwidth, message sending, and obtaining of users' address. Costs of bandwidth and message sending are ignorable. According to Sadowsky (2003, p. 55), the spammer could obtain users' e-mail address in 13 situations. Obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software, which is also available from Internet, either being free of charge or with an inexpensive price.

The revenue of spammer from sending message has been found high in a few studies (Goodman and Routhwaite 2004). Cobb (2003, p. 2) suggested the concept of "the parasitic economics of spam," meaning that the act of sending a message cost the sender less than it cost all other parties impacted by sending of the message.

Costs and benefits of the spammed can also be estimated. Costs induced by spam to the spammed have a wide coverage, including waste of users' time, bandwidth and storage, cost of anti-spam solution, and cost of overloading at the mailbox (Gauthronet and Drouard 2001). The average time and money lost in processing a single message might not be so significant. However, theoretically, aggregate losses of time and money taken in dealing with these messages might be huge (Li 2006). Spam also induces costs of bandwidth and storage, losses in interruption of services, and anti-spam solutions (Gauthronet and Drouard 2001). Interruption of services is unfortunate for both providers and users in causing business, confidence, and other losses. Worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC 2005). If e-mail address has ever been put on institution's Web site, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by senders (Federal Trade Commission 2003b).

Finally, unsolicited e-mail is nothing useful and beneficial to recipients. From all of the previous studies, it is reasonable to conclude that recipients undertake pure losses, not only the monetary, but also the psychological (Li 2006).

Methodology

The paper presents a case study on UEMAs, analysing the sender column, subject column, content and attachments of these message. Two samples were used, one was composed of 501 messages, and the other was composed of 490 messages, with attachments out of total approximately 78,820 unsolicited e-mail messages received in an e-mail account during June 2005 to March 2008. When the sample was taken, UEMAs constituted 19.2 ‰ of all the 26,160 unsolicited e-mail messages. When the second sample was taken, they constituted 9.3 ‰ of 56,750 unsolicited e-mail messages collected during the same period. Figure 1 gives a snapshot of the e-mail account, showing the quantity of messages.

The account has received 78,910 messages in total, with normal messages accounting for a small proportion20and 78,820nsolicited messages in folders "research "research1, "501and "490. 501 UEMAs have been collected in folder "510.The 490 UEMAs have been collected in folder "490." The first sample, which constituted the framework of this study, was analyzed in May 2006. The second

sample, analyzed in March 2008, was primarily used to supplement the previous findings.

§

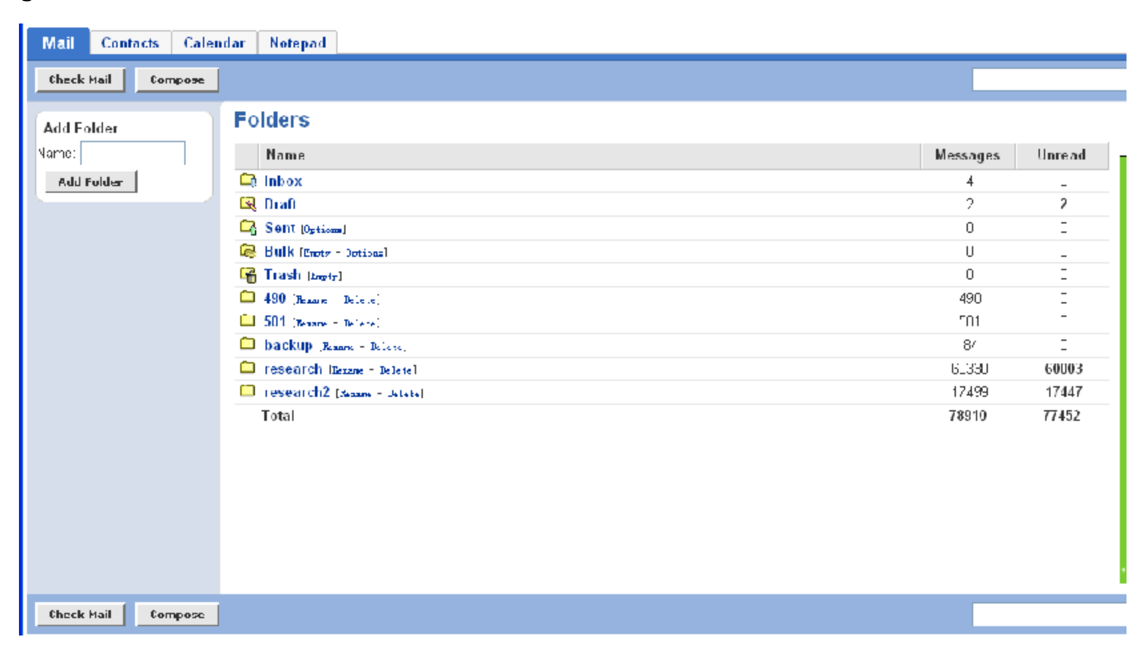


Figure 14 Snapshot of the e-mail account showing the quantity of messages (as of 30 March 2008)

Because of the private nature of this e-mail account, it is easy to judge which message is unsolicited. In analysing each message, it is necessary to establish a standard to categorise messages into different types according to their sender column, subject column, content and attachments. The standard to decide if the sender column is falsified is the name format. The name for an organization is also easy to judge by comparing the name in the sender column with that in the content.

The standard for deciding whether a subject column is falsified can be loosely defined. Because there is only one message labelled with an "AD:" sign, in strict sense all the subject columns of other messages are illegal. However, the emphasis of this paper is not to coincide with the legal standard. Rather, it is focused on analysis of phenomena of UEMAs. The message with "AD:" label and messages with words explaining the content or having apparent connection with the content are regarded as not falsified. Other messages with subject column irrelevant with the content, inducing recipient to open messages, is considered falsified. The content is categorised according to offers provided, and the nature of attachments. Analysis of both samples is presented in this paper. Sections about validity of sender column, subject column and content of UEMAs are primarily based on the first sample.

Limits of this study are that the resource account was not broadly put on the Internet, but was published on only one website specialised on traditional publishing service, to soliciting submission of academic articles. It is difficult to determine whether a random sample of all UEMAs sent in the stream of commerce would yield similar findings. It is also unknown that whether publishing- and printing-related UEMAs are due to the resource specialisation.

Findings

Types of File Formats of Attachments

In the first sample of 501 UEMAs, three attachments were missing. Other attachments were comprised of 14 kinds of document formats. More than one third of attachments were "zip" format compressed files, mostly viruses, which represented the most severe threats to the e-mail users' computer security. Another one third of all attachments were comprised of two categories: approximately one fifth of the total attachments being "gif" format image files, and approximately one sixth being "htm" format documents. This one third was relatively virus free, but included annoying contents and hyper links. These three kinds of files constituted more than 70 percent of all attachments. Another frequent attachment format was Microsoft Word "doc", which accounted for 8.4 percent of all attachments. Other 10 kinds of document formats were only responsible for approximately 20 percent of attachments, including both viruses and virus free files.

Three of the second sample of 490 UEMAs lost their attachments. Other 487 messages had 496 attachments, which included more types of files than in the first sample. Text files and "gif" files accounted for nearly 70 percent of these attachments. The most obvious change happened in growing role of text files and declining role of "zip" files, from which I observed that the use of UEMAs had become more rational in advertising practical information other than in spreading viruses. This conclusion was also supported by the decrease of executable files or their disguised formats, such as "com," "exe," "pif," "scr," and so on. Another observable change was that "html" files decreased by nice percent in attachments. In both samples, "gif" files had a significant percentage, but in fact, they were usually small, benign and meaningless. In sum, types of attachments took on a diversified outlook, with files of familiar formats changing to rational advertisements, and

malicious motives seeking unfamiliar formats, at a satisfactorily smaller overall scale.

Table 3 Types of File Formats of Attachments

(In second sample, some messages had multiple attachments)

		Attachments in first sample		Attachments in second sample		Change of types
	Types of File Formats	Number	Percentage	Number	Percentage	Percentage
1	*.chm	11	2.2	4	0.8	-1.4
2	*.com	9	1.8	2	0.4	-1.4
3	*.doc	42	8.4	40	8.1	-0.3
4	*.exe	13	2.6	5	1.0	-1.6
5	*.gif	92	18.5	129	26	+7.5
6	*.htm	78	15.7	32	6.5	-9.2
7	*.jpg	13	2.6	12	2.4	-0.2
8	*.mid	3	0.6	0	0	-0.6
9	*.pif	19	3.8	1	0.2	-3.6
10	*.rar	11	2.2	16	3.2	+1.0
11	*.scr	12	2.4	4	0.8	-1.6
12	*.txt	8	1.6	216	43.5	+41.9
13	*.xls	3	0.6	2	0.4	-0.2
14	*.zip	184	36.9	12	2.4	-34.5
15	*.epf	0	0	1	0.2	+0.2
16	*.hqx	0	0	10	2.0	+2.0
17	*.ini	0	0	1	0.2	+0.2
18	*.pdf	0	0	1	0.2	+0.2
19	*.png	0	0	1	0.2	+0.2
20	*.rtf	0	0	2	0.4	+0.4
21	*.url	0	0	2	0.4	+0.4
22	*.uu	0	0	3	0.6	+0.6
	Messages with missing attachment	3		3		
	Total attachments	498	100	496	100	

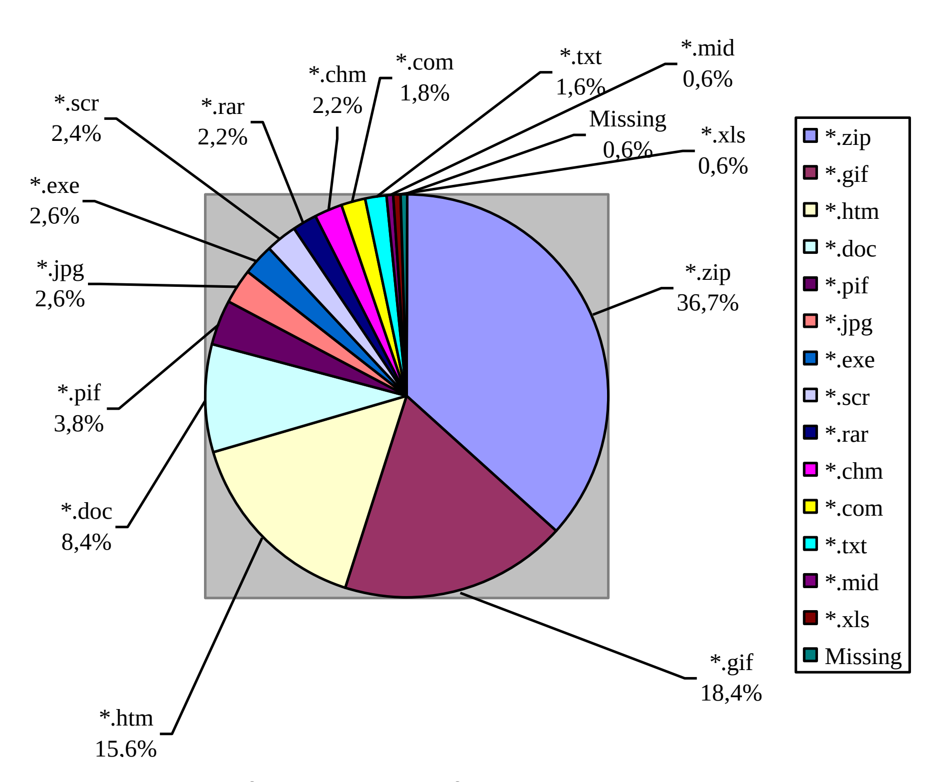


Figure 15 Types of File Formats of Attachments in 2006 Sample

Sizes of UEMAs

The average size of messages in the first sample was 47.44kb. Sizes of approximately 90 percent of UEMAs were smaller than 100kb. Sizes of only 2 percent of these messages were between 100-200kb. Sizes of nearly 9 percent of messages were bigger than 200kb. In fact, about 285 pieces of messages, which constituted more than half of UEMAs, were smaller than 30kb. Messages with the sizes of 1kb and 2kb alone accounted for more than 28 percent of the sample. They were mostly empty "zip" files with the possibility of being UEMAs of viruses but disinfected by e-mail service providers. UEMAs spreading W32.netsky.C@mm (35k) and W32.Sober.X@mm (75) viruses accounted for 16 percent and 7 percent of all of messages respectively.

In the second sample, the average size was 76.53kb, about 61 percent bigger than that of the first sample. UEMAs smaller than 100kb constituted almost the same percentage as in the first sample. About three percent more messages were between 100 and 200kb, and fewer messages were bigger than 200kb. Nearly 70 percent of messages are smaller than 30kb. UEMAs smaller than 1kb and 2 kb apparently decreased in the second sample, accounting for only 6 percent.

Table 4 Sizes of UEMAs

	Massages in the first sample		Massages in the second sample	
Size	Numbers	Percentage	Numbers	Percentage
‹100kb	446	89.0	424	86.5
100-200kb	11	2.2	26	5.3
›200kb	44	8.8	40	8.2
Total size	23,765kb		37,500kb	
Average size	47.44kb		76.53kb	
Among which				
‹30kb	285	56.7	377	76.9
1kb	13	2.6	3	0.6
2kb	108	21.6	25	5.1
35kb	80 (Virus: W32.Netsky.C@mm)	16		
75kb	35 (Virus: W32.Sober.X@mm)	7		
40-45kb			3 (Viruses: W32.Blackmail.E@mm!enc, W32.Lovgate.R@mm)	0.6

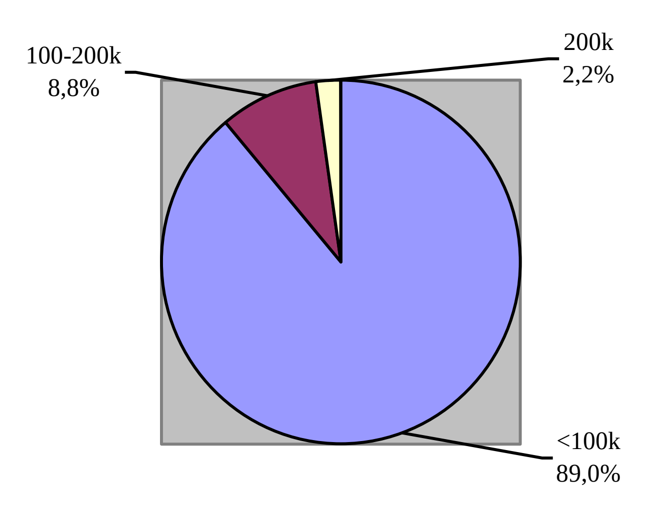


Figure 16 Sizes of UEMAs in 2006 Sample

In the first sample, UEMAs accounted for less than 2 percent of all unsolicited messages. The average size of unsolicited e-mails with attachments was 47.44kb, compared with the average size of 7.32kb of other unsolicited e-mails, a 6.5 fold bigger. In fact, UEMAs contributed to more than 10 percent of the average message size of all unsolicited messages, enlarging the average size from 7.32kb of unsolicited messages without attachments to 8.09kb of all of the unsolicited messages. When calculating message sizes in the second sample, I found that the average size had significantly enlarged, since there were 8 messages with the size ranging from 1mb to 4mb. These messages alone contributed to an average of 31.8kb for all the messages in the sample. Interestingly, large-sized messages were usually sent by political-oriented groups with the intent to spread political speeches.

Table 5 Compare of Average Sizes of Messages in 2006 Sample

	Total size	Numbers	Average size
Average size of unsolicited e-mails with attachments	23,765k	501	47.44k
Average size of other unsolicited e-mails	186,254k	25,459	7.32k
Average size of all unsolicited e-mails	210,019k	25,960	8.09k

Types of Sender Columns in UEMAs

Among the 501 pieces of UEMAs, one is with a blank sender column. Senders of UEMAs tend to hide their names but show e-mail addresses, valid or false. Approximately 60 percent of all messages show e-mail addresses instead of senders' name, which should be considered substandard. Others conceal their names with their surnames and titles, meaningless letters and numbers, describing their offers (products, services and activities), filled with words inducing users to open messages, or simply exploiting recipients' names and e-mail address. In total, approximately 83 percent of messages bear substandard sender columns. Only around one sixth of messages bear standard personal names or company names.

Table 6 Types of Sender Columns in UEMAs

	First sample		Second sample		Changes in percentage
Types of sender columns	Number	Percentage	Number	Percentage	
Blank	1	0.2	1	0.2	0
Company name	45	0.9	27	5.5	+4.6
Describing products, services and activities	16	3.2	136	27.8	+24.6
Inducing users to open messages	7	1.4	14	2.9	+1.5
Meaningless letters and numbers	23	4.6	105	21.4	+16.8
Recipients' name and address	4	0.8	1	0.2	-0.6
Showing e-mail address	297	59.3	72	14.7	-44.6
Standard personal name	79	15.8	86	17.6	+1.8
Surname plus title	29	5.8	48	9.8	+4.0
Total	501	100	490	100	

In the second sample, messages with sender columns describing products,

services and activities increased by a quarter. Messages with sender columns comprised of meaningless letters and numbers increased by nearly 17 percent. Showing e-mail addresses in sender columns decreased nearly 47 percent.

Valid Sender Columns in UEMAs

With the first sample, I analyzed in more details validity of sender column, subject column, and content. The following sections are primarily based on the first sample. Senders of UEMAs that were currently empty, or with the content of offering banking or financial services, sales of falsified certificate, human resources recruitment, publishing and printing, sales of health products and clothes, soliciting friends, and with the purpose of merely spreading computer viruses were reluctant to provide sender names in standard formats. Senders of UEMAs who offered telecommunications services were also quite reluctant to do so. Approximately one in every three senders of UEMAs offering information on companies and websites, sales of books, VCD and DVD provided valid name format in sender column. Half of quick money opportunities providers typed right names in their messages' sender column. Senders of UEMAs that offered tax evasion assistance seemed more active in providing standard format of names in the sender column. More than half of them did so. Sixty percent of senders who offered information on training and education opportunities typed names in standard format in the sender column. The providers of computer hardware and software appeared the most reliable senders of UEMAs, of whom more than 70 percent furnished standard sender column. One quarter out of senders who offered other services gave valid form of names.

Table 7 Valid Sender Columns in UEMAs in 2006 Sample

Type	Number of validity in sender column	Percentage
Banking, financial	0	0
Empty attachments	0	0
Falsified certificate	0	0
Human resources recruitment	0	0
Introduction of	6	33.3

company, website		
Political propaganda	14	56
Publishing, printing, card manufacture, etc.	0	0
Quick money	1	50
Sales of books, VCD, DVD	4	36.4
Sales of health products, clothes	0	0
Software, computer products	33	70.2
Soliciting friends	0	0
Tax evasion	37	53.6
Telecommunications services	1	3.4
Training and education	6	60
Virus	0	0
Other services	1	25

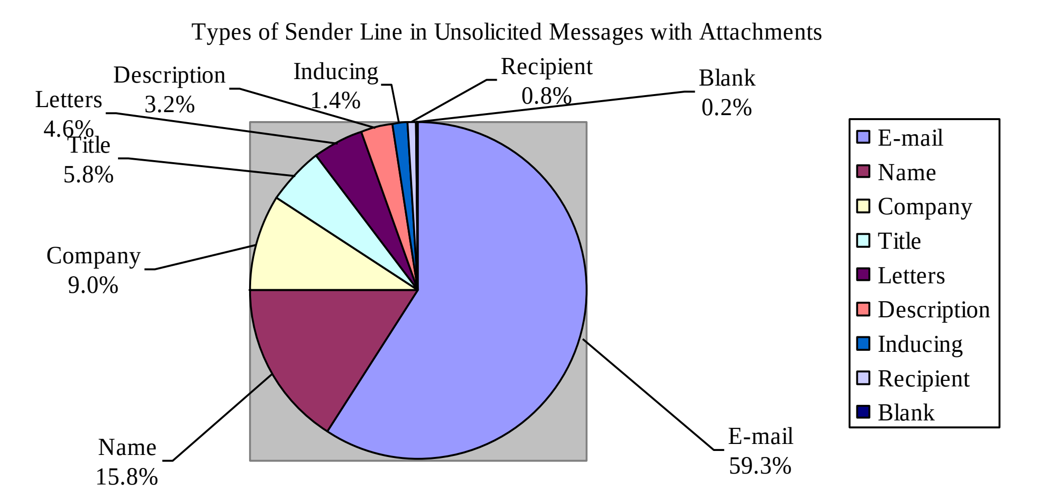


Figure 17 Types of Sender Columns in UEMAs in 2006 Sample

Types of Subject Columns in UEMAs

To label the subject column with “AD:”, “ADV:”, or any other kinds of regulatory means, was an invention that had never been respected by senders of

unsolicited messages. According to calculation of the first sample, only less than two in one thousand messages had this kind of label. Two in one hundred of UEMAs left the subject column blank. More than 17 percent of messages used ambiguous wording to confuse recipients, or other particular terms attempting to draw recipients' attention and attracting them to open messages, furnished the subject column with languages describing the content, giving greetings, appearing related to users' e-mail service, bearing "To:", "Re:" and "Fw:" labels, or pretending users' friends and contacts, etc. The hacking tactics of so-called social engineering was to a great extent used in these messages. In the second sample, messages with subject columns describing message content increased by nearly 50 percent, while messages with subject columns pretending to be recipient's contact decreased by more than 40 percent.

Table 8 Types of Subject Columns in UEMAs

	First sample		Second sample		Change in percentage
Type	Number	Percentage	Number	Percentage	
"AD:" label	1	0.2	0	0	-0.2
Attractive wording	87	17.4	26	5.3	-12.1
Blank	10	2	8	1.6	-0.4
Describing message content	117	23.4	354	72.2	+48.8
"To:", "Re:" and "Fw:" label	21	4.2	25	5.12	+0.92
Users'	2	52.9	4	8.98	-

friends and contacts	65		4		43.92
Other	0	0	3 3	6.7	+6.7
Total	5 01	100	4 90	100	

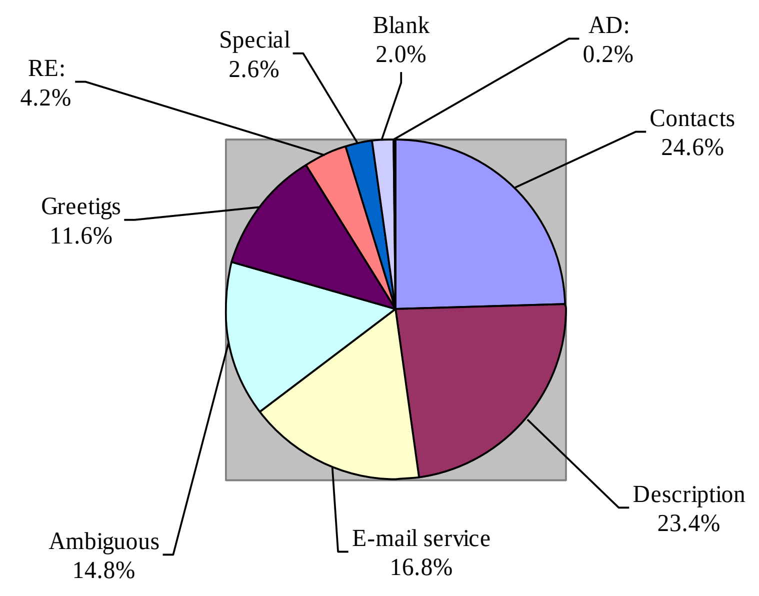


Figure 18 Types of Subject Column in UEMAs in 2006 sample

Valid Subject Columns in UEMAs

Almost all of senders of UEMAs offering information on human resources recruitment, companies or websites, publishing, printing, card manufacture, etc., sales of health products, clothes, and tax evasion ensured the valid subject column. A high percentage of providers of telecommunications services, sellers of books, VCDs, and DVDs, training information providers, quick money information providers, and providers of other services provided valid subject columns in their messages. All senders of other messages were reluctant in typing useful subjects for their potential recipients.

Table 9 Valid Subject Columns in UEMAs in 2006 Sample

Type	Number	Perce ntage
Bank, financial	0	0
Empty attachments	11	10.7
Falsified certificate	0	0

Human resources recruitment	2	100
Introduction of company, website	18	100
Political	1	4
Publishing, printing, card manufacture, etc.	19	100
Quick money	1	50
Sales of books, VCD, DVD	8	72.7
Sales of health products, clothes	4	100
Software, computer products	1	2
Soliciting friends	0	0
Tax evasion	66	95.6
Telecommunications services	24	82.8
Training	7	70
Virus	0	0
Other services	3	75

Types of Content of UEMAs

More than 28 percent of messages were designed to spread viruses. More than one in five messages attached empty attachments. Messages offering both tax evasion services and software and computer products constituted around 10 percent of all messages. Any of contents of other messages constituted a percentage far below 10 percent, with messages offering telecommunications services and political propaganda constituting around 5 percent separately. Interestingly, there was rarely any message with attachment involving adult contents, investment chances, sales of pirated software, and some other common offers in messages without attachments.

Table 10 Types of Content of UEMAs in 2006 Sample

Type	Number	Percenta

		ge
Bank, financial	3	0.6
Empty attachments	103	20.6
Falsified certificate	10	2
Human resources recruitment	2	0.4
Introduction of company, website	18	3.6
Political	25	5
Publishing, printing, card manufacture, etc.	19	3.8
Quick money	2	0.4
Sales of books, VCD, DVD	11	2
Sales of health products, clothes	4	0.8
Software, computer products	47	9.4
Soliciting friends	4	0.8
Tax evasion	69	13.8
Telecommunications services	29	5.8
Training	10	2
Virus	141	28.1
Other services	4	0.8

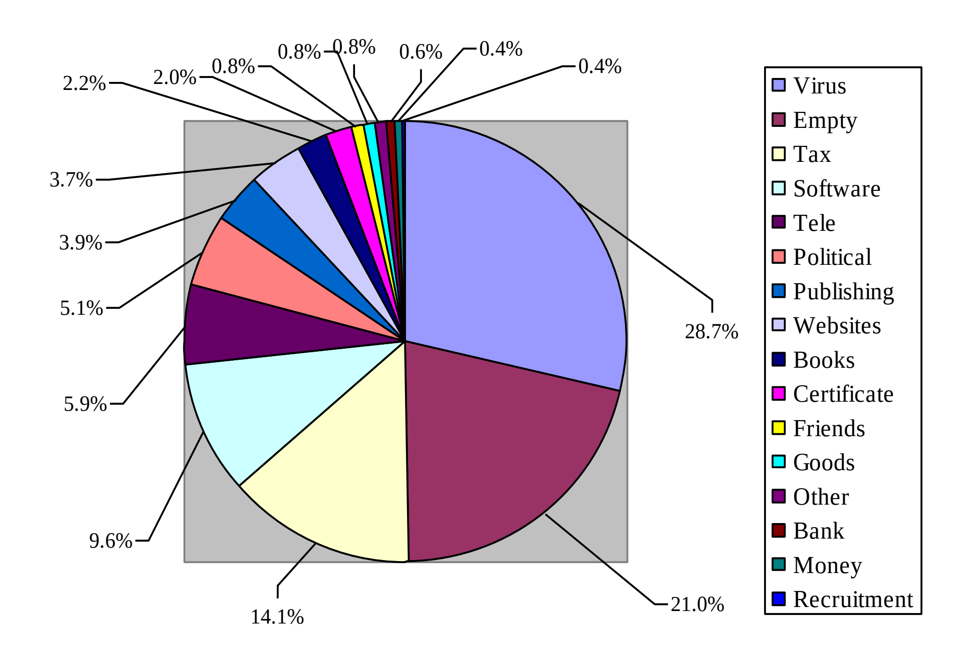


Figure 19 Types of Content of UEMAs in 2006 Sample

Valid Content in UEMAs

Interestingly, most messages had high percentage of valid contents, with exception of messages with empty attachments and UEMAs that spread viruses.

Table 11 Valid Content in UEMAs in 2006 Sample

Type	Number of validity in content	Percentage
Bank, financial	0	0
Empty attachments	0	0
Falsified certificate	9	90
Human resources recruitment	2	100
Introduction of company, website	13	72
Political	25	100
Publishing, printing, card manufacture, etc.	19	100
Quick money	1	50
Sales of books, VCD,	11	100

DVD		
Sales of health products, clothes	4	100
Soliciting friends	4	100
Software, computer products	47	100
Telecommunications services	24	82.8
Training	8	80
Virus	0	0
Other services	1	25

Types of Contact Methods Provided in UEMAs

Because many UEMAs were spreading viruses, they generally provided no contact information, with a few exceptions. Other messages included one or more kinds of contact methods in the message texts. Of total 501 messages in the first sample, more than one-third of messages provided hyperlinks directed to websites, while less than one-third provided fixed telephone numbers. Both e-mail addresses and mobile phone numbers were preferred by more than 22 percent of senders. Fax numbers and physical addresses were included in about 16 and 10 percent of messages separately. QQ (a chat system) were provided in 8 percent of messages. MSN was the least used contact method in the 501 messages.

Unsubscribe is nothing more than a decoration in UEMAs. Unsubscribe method was only provided in 2.2 percent of messages in the first sample.

Table 12 Types of Contact Methods Provided in UEMAs in 2006 Sample

Contact Methods	Number	Percentage (/501)
Address	50	10
E-mail	113	22.6
Fax	79	15.8
MSN	12	2.4
Mobile phone	112	22.4
QQ	40	8

Telephone	145	28.9
Unsubscribe method	11	2.2
Website	182	36.3

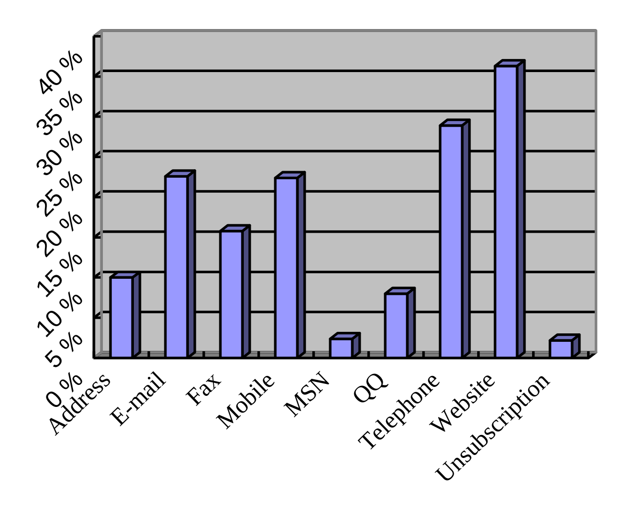


Figure 20 Types of Contact Methods Provided in UEMAs in 2006 Sample

Falsity of Sender, Subject and Content

In the first sample, only one in five of UEMAs used valid format in sender column, one in three used valid subject column, and more than half provided valid content. However, only 58 messages had both valid format of sender and subject column, and 293 messages with both false format of sender and subject column. Other 42 messages had valid format of sender column but false format of subject column, while 108 messages had false format of sender column but valid format of subject column. The overall falsity of subject or sender column constituted 88.4 percent.

Table 13 Validity and Falsity of Sender and Subject Columns and Content Separately

		Number	Percentage
Sender	Valid	100	20
	False	401	80
Subject	Valid	166	33.1
	False	335	66.9
Content	Valid	260	51.9
	False	241	48.1

The validity and falsity of content took almost 50 percent separately.

Table 14 Validity and Falsity of Either Subject or Sender Columns

		Sender			
		Valid	False	Total numbers	Percentage
Subject	Valid	5	1	16	33.1
	False	4	2	33	66.9
	Total numbers	100	401	501	100
	Percentage	20	80	100	
	Percentage of validity of both columns	11.6			

Discussion

In activities of sending unsolicited e-mail messages, one of the most important aspects is to induce recipients to open and read messages and their attachments. Senders of UEMAs took particular considerations in disguising their real identity and real purpose. It can be said that most of them demonstrated a high degree of skill in motivating recipients to open messages and their attachments. However, opening messages and attachments was usually the first step towards for senders to victimize other users. Generally, they used ambiguous wording in sender and subject columns but valid content (except messages spreading viruses) so as to ensure messages and attachments be open and advertisements be read.

Analysis of the two samples roved that, except messages deliberately spreading viruses, UEMAs were usually less harmful than it was found in findings of previous studies that did not distinguish UEMAs from those without. It implied that senders of unsolicited e-mail messages tended to transform their product or service information.

At the same time, this study revealed that UEMAs could have broader negative

impact on criminal phenomena, not only victimization, but also conspiracy. E-mail communications could be taken as an offensive means by which recipients were victimized, or a conspiracy tool with which recipients were seduced to commit crimes. UEMAs that spread viruses could directly result in victimization of recipients, their computers damaged or manipulated, or their secret or privacy stolen or disclosed. Some UEMAs could move recipients to invest their money to projects that could never generate any reward. Some UEMAs could victimize recipients in crimes that recipients being physically or sexually attacked. Or, these messages could induce recipients to collaborate on some criminal plots.

In cyber environment, the most frequent victimization model began from exposing of victims to potential threats, which we can label as exposing-victimization model. Under this model, the victim of UEMAs exposed their addresses merely on web pages, in bulletin board systems (BBSes), in chat systems, or simply in transmission through the Internet. Exposure on the Internet does not necessarily mean show-off. Rather, it should have been a usual kind of digital presence. Nevertheless, the exposing-victimization model at least implies that senders of UEMAs could easily harvest e-mail addresses in the same way as normal Internet users do

In other cases, senders of UEMAs had a seeking process, and followed the seeking-victimization model. Due to the large quantity of web pages and other Internet-related contents, direct artificial collection of multiple e-mail addresses became inefficient. By making use of specialized software to harvest e-mail addresses from the Internet, senders could collect millions of addresses automatically in a short time. By doing so, they created the seeking-victimization model in sending UEMAs. Besides harvesting, they also exploited dictionary attack and/or automatic alphabetical permutation and combination to enumerate possible usernames in e-mail accounts. All of these methods could be used in seeking process. For senders, an e-mail account with a random word might not represent a specified person; but for the recipient, he/she would readily be the potential victim of this UEMA.

Victimization of recipients of UEMAs could happen without recipients accessing their e-mail accounts. Their victimization resulted from their e-mail accounts being spammed, whether they accessed their accounts or not. Under current legal framework, receiving of unsolicited messages is sufficient to be regarded as victimization caused by acts that imposed punishment by law.

However, victimization of UEMAs does not end at the initial victimization. The

above-mentioned models could be called as the first level effects of UEMAs. The second level effects could take place on basis of the initial victimization. There could also be two sub-models: victimization-victimization sub-model and victimization-conspiracy sub-model.

The victimization-victimization model happened when messages spread viruses, fraudulent sales of goods, or falsified financing and banking services. The first level victimization was for recipients to be spammed, while the second level victimization was for recipients to be attacked or swindled upon opening the malicious programs or following the fraudulent scams.

The second level victimization would not always be accomplished so straightforwardly. Usually involved was a victimization-exposing-seeking-victimization process. The most typical scam of this kind was Nigerian fraud (or 419 fraud), in which recipients of unsolicited messages were firstly victimized by receiving this kind of messages (being spammed). If they made a positive reaction to messages, they were further exposing their vulnerabilities to senders. Upon receiving reply from recipients, senders would further seek vulnerabilities of recipients and at last obtain their property. The process of seeking and exposing might be a long interaction between senders and recipients, who exchanged messages until the final transaction. If senders succeeded in obtaining recipients' property, the last victimization would take place and the scam would come to an end.

The victimization-conspiracy model happened when messages included assistance for tax evasion services, sales of pirated software, sales of falsified documents, and so on. Recipients of such offer were firstly victimized by unsolicited messages; and if they participated in illegal operations, they would become conspirators of senders.

Because recipients of unsolicited messages inducing conspiracy in an illegal operation would expect to have the luck to benefit from collaborating with senders who pretended to have the potential to give charity, senders were more likely to send this kind of messages. In fact, in Nigerian fraud, senders were usually personating politicians who want to transfer property (money, diamond, and so on) to bank accounts of recipients by claiming to give a significant reward. As a result, recipients, who wished they could have been "conspirators" in a great operation of money laundering, would finally be victimized in scams that they lost advance fees.

Conclusion

Phenomena of UEMAs further proved the low controllability or uncontrollability of cyber environment. Exposed e-mail addresses are vulnerable to unsolicited messages. Unexposed e-mail addresses can be as vulnerable as exposed ones, because address harvesting software can collect potential addresses from transmission route of the Internet. As far as our study is concerned, this process makes extra sense. For senders, both ways could be seen as a process of seeking vulnerabilities. For recipients, both ways could also be seen as a process of exposing vulnerabilities. However, seeking and exposing process has become more abundant and colourful in cyber environment than pre-Internet times.

Mere browse of web pages is the easiest method to obtain e-mail accounts, but it is less efficient because e-mail addresses are usually scattered in many different pages. This process would be time-consuming if thousands or millions of addresses are to be collected. Senders can also purchase millions of addresses of users with different interests from specific vendors, who have the best method and specialized personnel to harvest addresses from all over the cyberspace, and usually establish their own databases of addresses. With an inexpensive price, buyers can conveniently get a large quantity of addresses. In addition, address harvesting becomes automated and prevalent with the help of specified software. Many people who are interested in doing spamming business can easily master uncomplicated skills and collect millions of addresses with such software, which can be downloaded from the Internet free of charge or with a small payment.

Exposing e-mail addresses on the Internet is literally unavoidable, because the exposure is in so broad a sense that all the normal use of e-mail services could be seen as an exposing process, including sending and receiving messages; publishing on web pages, chat rooms, and BBSes; providing as register information in online services; or exposing nothing but coincidence with a dictionary vocabulary; and so on. In fact, exposing a single e-mail account will not be so risky if there is not such a thing as address harvesting technique, because it is an inefficient way to collect single e-mail account one by one from the Internet. However, we cannot simply ignore such a method because e-mail account vendors could collect and transact addresses in a dynamic process, and collect addresses through a variety of ways to establish their databases. Address harvesting software and dictionary attack undoubtedly intensify

the victimization of e-mail account holders.

In general, exposed e-mail accounts might face double risks of being victimized: being collected in process of formally browsing web pages and use of other Internet services; and being harvested during the process of digital transmission or merely guessed by senders through randomly combining letters and numbers. Compared with daily used e-mail accounts without exposing on web pages or other Internet services, published accounts are more likely to be spammed. Therefore, it seems more likely that vendors or senders harvest addresses with automated technique. As a result, double risks of exposed e-mail accounts are in fact unbalanced: the risk of being victimized by collectors and harvesters are far serious than that by guessers.

UEMAs provide e-mail users many different choices, either conspiring in criminal acts, or victimized by viruses or in scams. Messages analyzed in this study generally gave recipients two alternatives: conspiring in tax evasion, or damaged by viruses.

In the case of conspiracy in tax evasion, senders used to provide valid contact methods so as to induce recipients to participate in illegitimate operations. The offer seemingly aims to establish a relationship between tax evasion service provider and their potential clients. However, the effect was that they form conspiracy in tax evasion activity. Recipients had to react actively before they become conspirators of tax evasion activities. The process might involve repeated e-mail exchanges upon initial unsolicited messages. Under these circumstances, unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information for recipients. Thus recipients might tend to accept such messages and offers in them. Such messages become the communication means for criminals, posing great threats for social control over illegal activities.

In the case of viruses attack, senders exploited social engineering to induce recipients to open messages and their attachments, by blurring sender, subject columns and falsifying message content and file names of attachments. These messages did not require any reply from recipients before they caused damages. They were also dangerous for recipients in the sense that they were harming recipients' hardware and software, wasting time and labour.

References

Boldt, M., Carlsson, B., and Jacobsson, A. 2004. Exploring Spyware Effects. Retrieved 14 January 2009, from http://www.tml.tkk.fi/Nordsec2004/Presentations/boldt.pdf

Cobb, S. 2003. The Economics of Spam. Retrieved 14 January 2009, from http://www.spamhelp.org/articles/economics_of_spam.pdf

Fallows, Deborah. 2003. Spam: How It Is Hurting E-mail and Degrading Life on the Internet. Retrieved 14 January 2009, from http://www.pewinternet.org/pdfs/PIP_spam_Report.pdf

Federal Trade Commission. 1998. Federal Trade Commission Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, *Federal Trade Commission Consumer Alert*. Retrieved 14 January 2009, from http://library.findlaw.com/1998/Jul/1/128450.html

Federal Trade Commission. 2002a. *Remove Me Surf*, Author. Retrieved 14 January 2009, from http://www.ftc.gov/bcp/conline/edcams/spam/pubs/removeme.pdf

Federal Trade Commission. 2002b. E-mail Address Harvesting: How Spammers Reap What You Sow, Author. Retrieved 14 January 2009, from http://library.findlaw.com/2003/Aug/8/132973.pdf

Federal Trade Commission. 2003a. *False Claims in Spam: A Report by the Federal Trade Commission's Division of Marketing Practices*, Author. Retrieved 14 January 2009, from http://www.ftc.gov/reports/spam/030429spamreport.pdf

Federal Trade Commission. 2003b. *National Do-Not-E-mail Report to Congress*, Author. Retrieved 14 January 2009, from http://www.ftc.gov/reports/dneregistry/report.pdf

Gauthronet, S., and Drouard, E. 2001. *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General. Retrieved 14 January 2009, from http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/spamsum_en.pdf

Goodman, Danny. 2004. Spam Wars: Our Last Best Chance to Defeat Spammers, Scammers & Hackers, New York, New York: SelectBooks.

Goodman, J. T., and Rounthwaite, R. 2004. Stopping Outgoing Spam. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17-24 May, ACM Press, pp. 30-39. Retrieved 14 January 2009, fromhttp://research.microsoft.com/~joshuago/outgoingspam-final-submit.pdf

IDC. 2005. Worldwide Revenue for Antispam Solutions To Reach Over $1.7 Billion in 2008, IDC Reveals. *IDC - Press Release*. Retrieved 14 January 2009, fromhttp://findarticles.com/p/articles/mi_m0EIN/is_2005_Feb_24/ai_n10300118

Karnell, J. 2002. Raising the Stakes in Permission Marketing. Retrieved 14 January 2009, fromhttp://www.onetooneinteractive.com/resource/whitepapers/0003.html

Khong, W. K. 2001. The Law and Economics of Junk E-mails (Spam). Retrieved 14 January 2009, fromhttp://www.emle.org/Thesis/Khong.pdf

Khong, W. K. 2004. An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1 (February), 23–45. Retrieved 14 January 2009, fromhttp://www.eler.org/include/getdoc.php?id=8&article=2&mode=pdf&OJSSID=6170ccc598edb033fc0ccf2477a86ee9

Lambert, Anselm. 2003. *Analysis of Spam*. Master of Science in Computer Science Dissertation, Dublin: University of Dublin.

Li, Xingan. 2006. E-marketing, Unsolicited Commercial E-mail, and Legal Solutions, Webology, 3(1), Article 23. Retrieved 14 January 2009, fromhttp://www.webology.ir/2006/v3n1/a23.html

McWilliams, Brian. 2005. *Spam Kings*, Sebastopol: O'Reilly Media.

Nucleus. 2003. *Spam: The Silent ROI Killer*, Research Note D59. Retrieved 14 January 2009, fromhttp://www.spamhelp.org/articles/d59.pdf

Nucleus. 2004. *Spam: The Serial ROI Killer*, Research Note E50. Retrieved 14 January 2009, fromhttp://tim.blog.kosmo.com/article_files/NucleusResearchCostOfSpam.pdf

Organization of Economic Cooperation and Development. 2003. *Organization of Economic Cooperation and Development Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author. Retrieved 14 January 2009, fromhttp://www.oecd.org/document/56/0,2340,en_2649_34267_2515000_1_1_1_1,00.html

Organization of Economic Cooperation and Development. 2004. *Second Organization of Economic Cooperation and Development Workshop on Spam: Report of the Workshop*, Author. Retrieved 14 January 2009, fromhttp://www.oecd.org/dataoecd/55/32/31450810.pdf

PC World. 2003. Sobig May Be Working for Spammers. Retrieved 14 January

2009, from http://www.pcworld.com/news/article/0,aid,112261,00.asp

Radical Group. 2005. *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*, Author. Retrieved 14 January 2009, fromhttp://www.radicati.com/uploaded_files/news/Q1-2005_PressRelease.pdf

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., and Schwartz, A. 2003. *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.

Simon, H. A. 1982. *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. Massachusetts: Massachusetts Institute of Technology Press.

Sorkin, D. E. 2001. Technical and Legal Approached to Unsolicited Electronic E-mail, *University of San Francisco Law Review*, Vol. 35, pp. 325-384. Retrieved 14 January 2009, fromhttp://www.sorkin.org/articles/usf.pdf

Spammer-X. 2004. *Inside the SPAM Cartel*, Rockland, Massachusetts: Synergies Publishing.

Taylor, Humphrey. 2003. Spam Keeps on Growing. Retrieved 14 January 2009, fromhttp://www.harrisinteractive.com/harris_poll/index.asp?PID=424

Trans Atlantic Consumer Dialogue (TACD). 2003. *Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam)*, Author. Retrieved 14 January 2009, fromhttp://www.tacd.org/db_files/files/files-296-filetag.doc

World Summit of Information Society. 2003. *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*, Author. Retrieved 14 January 2009, fromhttp://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

Federal Trade Commission. 2005. Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Prectices, November 2005, 10 pp. Retrieved 14 January 2009, fromhttp://www.ftc.gov/opa/2005/11/spamharvest.pdf

Chapter VI Critical Factors in Combating Cybercrime

Abstract

Fight against cybercrime necessitates better knowledge about the characteristics of cybercrime. The article is designed to make a synchronic inquiry into the characteristics of cybercrime in comparison with traditional offences. The article identifies a number of factors that complicate the reporting, detection, investigation, prosecution, conviction, and sentencing of cybercrime. The themes explored in this paper show that there is no easy way of bringing cybercriminals before the judicial process. Nevertheless, the increase of cybercrime is constant, and the reinforcement of deterrence is a constant need, yet for these two forces to reach equilibrium is still an on-going process.

Keywords: critical factors, combating cybercrime

Introduction

Alternative definitions of cybercrime have emerged over the years as the users and abusers of computers expand into new areas. There is neither a unified definition, nor a commonly accepted method of classification. The definition and classification methods are so diversified that it is impossible to sketch the scenario of cybercrime by using a single standard (Wasik 1991, p. 1). Before the 1990s, computer crimes were generally understood as offences relating to computers, but there was less connection with networks, even though the perpetrators of earlier computer crimes also exploited the networks. The situation in the pre-Internet age should easily be realized from the present viewpoint. However, the most noteworthy dispute then revolved around whether there was a distinct criminal phenomenon of computer crime. Roughly, three different standpoints existed. From the first standpoint, there was no such thing as computer crime (Johnson 1985; Gotternbarn 1990, pp. 18-24). The second standpoint claimed that the computer could be used to perpetrate every kind of crime (Nycum 1983, pp. 2-4; Donn B. Parker's view in Sterling 1994; Li 1993). The third standpoint was held by middle-of-the-roaders, who admitted the

existence of computer crime on the one hand, but limited the range of offences on the other.

Computer crime has been defined in a diverse spectrum of senses, from extremely narrow ones to extremely broad ones. The definition in the narrowest sense limits computer crime to "one that can be carried out only through the use of computer technology" (Tavani 2000, pp. 6-7). This definition excludes crimes that can be committed only through other means than computer technology and that can be committed in both ways. A broader approach defines computer crime as crime by computer. This definition excludes crimes targeting a computer. A yet broader definition includes both crimes by computer and against the computer (See, for example, McConnell International 2000; Reece 2000; See also Berg 2000; Goodman 1997, pp. 465, 468-469). The current view about offences against computers is likely to relate the physical forms of computers or computer technology to the function of computers. The broadest definition was proposed by Parker (1980, cited in Solarz 1981, pp. 25-26), who divided computer crimes into computer abuse, computer crime and computer-related crime. Obviously, the computer crime conception at the second level was included in the first level. The computer crime conception at the first level was extremely broad. In fact, Parker and Nycum (1984, p. 313) defined computer crime "as any illegal act where a specific knowledge of computer technology is essential for its perpetration, investigation, or prosecution," saying subsequently that computer crime was not regarded as a distinct type of crime different from other crimes, and that almost every sort of crime could be committed through the exploitation or intervention of computers (ibid). Such kind of a definition has accepted and developed by many subsequent studies (for example, Pihlajamäki 2004, p. 286).

In the network environment, the model of a computer crime becomes more relevant with the emergence of the Internet. Cybercrime is loosely defined as a crime committed by means of the computer or the Internet (Levinson 2002, p. 455). The Council of Europe Convention on Cybercrime 2001 made the term "cybercrime" prevalent. Articles 2-10 of the Convention on Cybercrime also adopted a broad conception in criminalizing cybercrime, providing for the offences against security, computer-related offences, and content-related offences. Although the Convention adopted a broad conception, the detailed offences under the titles were limited. The high level of consensus concerning conception, and the low level of consensus

concerning the categories is a factor that makes it reluctant for more countries to consider access to the treaty.

Some of the previous understanding about cybercrime has been misleading and confusing in providing inexact information. The first misunderstanding happened against a historical background, making the term “hacking” the equivalence of today’s “cybercrime”. A second misunderstanding of the conception takes it as a synonym of terrorism. The third misunderstanding is politicization of the conception in a broader sense. The fourth misleading understanding is, strangely, to moralize the cybercrime by exploiting the term “hacking”. The last category of misleading definitions has the tendency of mystification. The representative notion is that cybercrime is high-tech crime and does not seem to be committable by common users in daily life.

Cybercrime can be defined as any type or any form of traditional or untraditional crime involving information systems in use as media, means, place, route, target, tool, or used in the preparation for other crimes. Cybercrime covers any form of traditional or any type of untraditional crime that can involve information systems. Information systems are the distinct factor in cybercrime. Information systems must be in use. The roles of information systems in cybercrime are multiple.

Information systems have multiple vulnerabilities, plays multiple roles in cybercrime, while cybercriminals are themselves have varied motivations. This paper will discuss critical factors in the fight against such offences. The core question I seek to answer the question of the ease ordinarily in finding cybercrime. By saying “find”, I cover a wide range of activities leading to punishment: detection, reporting, investigation, prosecution, proving and conviction.

At present, the fight against cybercrime also necessitates better knowledge about the critical factors. For several decades, many commentators have written about the characteristics of cybercrime, and many aspects have been generalized in the light of the surveys, observation and thinking (Thompson 1989; Sieber 1998, etc.).

The paper is designed to make a synchronic inquiry into the characteristics of cybercrime in comparison with traditional offences.

The victims of cybercrime

The perpetrator-victim relationship in cybercrime is developed through information systems in a process of human-machine-human interaction. The perpetrator fulfils the first half of the interaction and the victim is imposed into the second half of the interaction. That is to say, the victimization of victims of cybercrime also relates to information systems. Victims are also users whose information is deposited in or published through information systems, whose daily life or operation depends on the systems, or whose welfare is increased through the systems. Like cybercriminals, they are also distributed over an unlimited area. In addition, in cases such as virus attacks, multiple victims can be involved. Thousands or millions of users are also likely to be victimized in one case even. Individual users usually have a lower awareness of cybersecurity than corporate users, and invest less money and time in maintaining and protecting the systems and less on updating their anti-virus software. Although individual users are more vulnerable to potential threats, their losses are usually neglected and underreported.

Computer networks are not so new, but the pervasive use of them is a recent development. The current generation of people accepts, and depends more on, information systems than previous generations. There exists a clear-cut information generation within the information society. Because more young people use the Internet than the elderly do, it is natural that these youths are more likely to be victimized in cybercrime. Thus to some extent cybercrimes are offences of youths against youths. We do not find a sharp reduction of computer use with the increase in the age of young users. Therefore, it is to be expected that with the increase in age of the Internet users, more victims will also be found in future among older users.

Simultaneously, it is undeniable that with more and more organizations pursuing online businesses and other activities, the likelihood that these organizations will be victimized will also grow. In fact, the victims of the original offences against information and information systems were mainly organizations. In the future, they will still be vulnerable to inside and outside attacks. One advantage these organizations have for protecting their information and information systems is that they have a greater capacity than the individual users to afford the anti-virus, firewalls, other access-control mechanisms and for updating these mechanisms.

It is a trickier question when the online victims are more likely to be victimized in a "voluntary" or "active" manner. For example, the Nigerian 419 fraud victims may transfer a sum of money voluntarily to the perpetrators; victims of date rape may

go to meet the potential criminals voluntarily; or users may voluntarily retrieve web pages that contain malicious codes, and so forth. Victims are also more likely to admit their "willingness" or "activeness" and less inclined to report the case.

Actual victimization in cybercrime can be more complex through the extension of victimization. For example, the senders of e-mail messages have adopted clever tricks in soliciting recipients. Opening the messages and the attachments is the first goal of the senders. Generally, they use ambiguous and false sender and subject columns, but ensure that there are valid contents (except messages spreading viruses) to show their offers and set their traps.

Unsolicited e-mail messages can have a broader influence on criminal phenomena, where the question is not only of victimization, but also one of conspiracy. Not only do e-mail communications become an offensive means by which the recipients are victimized, but these victims then serve as part of a conspiracy, for they are seduced to participate criminal operations.

In the Internet environment, the most frequent victimization model begins from an exposing of victims to potential threats, which we can call the exposing-victimization model. With this model, the victim of unsolicited messages merely puts his/her e-mail address on the web pages, bulletin-board systems, uses it in the chat systems, or even simply transmits it through the Internet. The exposure is not necessarily a show-off. Rather, it is just a kind of presence on the Internet literally or digitally, something inevitable. Nevertheless, the exposing-victimization model at least implies that the senders of unsolicited messages could easily get the e-mail address in the same way as other Internet users do, without further efforts in collecting or harvesting these addresses.

In other cases, the senders of messages have a search process, and follow the searching-victimization model. Due to the large quantity of web pages and other Internet-related contents, the direct artificial collection of multiple e-mail addresses becomes inefficient. The senders (here we also imply address providers) utilize specialized software to harvest e-mail addresses from the Internet. This collecting process becomes automatic and efficient. The perpetrators have created the searching-victimization model in sending messages. Besides harvesting, they also use a dictionary attack and/or an automatic alphabetical permutation and combination to enumerate possible usernames in e-mail accounts. These methods can also be categorized into a searching process. For the senders, an e-mail account with a

random word might not represent a specified person; but for the recipient, he/she is readily the victim of this unsolicited message with attachment.

The victimization of recipients of unsolicited messages happens without the appearance of the recipients in their e-mail account. The victimization means that their e-mail accounts are being spammed, whether they open their accounts or not. Under current the legal framework, the receiving of unsolicited messages is sufficient to constitute a victimization of the behaviour to be imposed punishment.

However, the victimization of unsolicited messages does not end at the initial victimization. The above-mentioned models could be called the first-level effects of unsolicited messages. Subsequently, the second-level effects are based on the initial victimization. There are possibly also two submodels: initial victimization-subsequent victimization model and initial victimization-conspiracy model.

The initial victimization-subsequent victimization model happens when the messages include viruses, fraudulent sales of goods, or falsified financing and banking services. The first-level victimization is being spammed, while the second-level victimization is being attacked or swindled.

Second-level victimization is not always fulfilled so simply. There is usually involved an initial victimization-exposing-searching-subsequent victimization process. In the case of the Nigerian 419 fraud, the recipients of the unsolicited messages were firstly victimized by receiving messages of this kind (being spammed). If they took a positive reaction to the messages, they were further exposing themselves to the senders. Upon receiving the recipients' response, the senders further worked on the vulnerability of the recipients and the possibility of obtaining their property. The process of searching and exposing might be repeated a number of times. If the senders succeeded in obtaining the recipients' property, the last stage of victimization would occur and the swindle would end.

The victimization-conspiracy model is realized when the messages include tax evasion services, sales of pirated software, sales of falsified documents, and so on. The recipients of such offers are firstly victimized by the unsolicited messages; and if they participating the illegal operations, they then become conspirators of the senders.

Because the recipients of the unsolicited messages inducing conspiracy in an illegal operation would expect to benefit from the cooperation with the senders, the senders are more likely to send attractive messages of the above kind. In fact, in

Nigerian fraud, the senders are usually personating politicians who want to transfer property (money, diamonds, and so on) to the bank accounts of the recipients. As a result, the "conspirators" of money laundering are finally to be victimized in the trickery.

The phenomenon of unsolicited e-mail messages has further proved the low controllability or uncontrollability of the information-network environment. Any e-mail address is vulnerable to unsolicited messages that are sent to exposed accounts on the Internet or to a supposed account according to the dictionary. For the senders, both ways could be seen as a process of searching. For recipients, both ways could also be seen as a process of exposing. However, these searching and exposing processes have become more abundant and colourful in the Internet environment than during pre-Internet times.

The mere browsing of the web pages is the easiest method to get an e-mail account, but it is less efficient. The sender can also purchase millions of addresses of different interests of users from the specific vendors. At an inexpensive price, the buyer can conveniently reach a majority of these addresses. Besides, address harvesting becomes automatized and prevalent with the help of powerful software. Anyone with a mild computer and Internet knowledge has the ability to master the uncomplicated skills and subsequently collect thousands or millions of addresses with specific software, which can be downloaded from the Internet free of charge or with a small sum of payment.

The exposure of an e-mail account on the Internet is unavoidable, because the exposure is in so broad a sense that everything in the normal use of the account could be seen as an exposing process, including the sending and receiving of messages; publishing on web pages, chat rooms, and BBSes; providing account information to register in online services; or exposing nothing more than a coincidence with a phrase from a dictionary vocabulary; or merely a permutation and composition of letters and numbers so that the senders are also fabricated. In fact, exposure of a single e-mail account will not be so risky without the harvesting mechanism, because it is an inefficient way of picking up a single e-mail account from the Internet. However, it cannot be ignored because the e-mail account vendors could collect and transfer it in a dynamic process, and finally form a growing account database to maintain their business. The harvesting software and a dictionary attack undoubtedly deepen the victimization of the e-mail account holders.

In general, the exposed e-mail account might face double risks of being victimized: being picked up in a formal browsing of web pages and use of other Internet services; and being harvested and guessed. Compared with daily-used e-mail accounts without showing up on the web pages or other Internet services except merely sending and receiving messages, the published accounts are more likely to be victimized. Therefore, it seems more likely that it is the process of harvesting rather than that of guessing is the one that the vendors of the database of e-mail accounts and senders of unsolicited messages feed on. As a result, the double risks of exposed e-mail accounts are in fact unbalanced risks: the risk of being victimized by collectors and harvesters is far more serious than the threats of the guessers.

Unsolicited messages provide e-mail users with several different choices, either legitimate or illegitimate, either to conspire or to be further victimized by attached viruses or pre-established fraud traps. The majority of messages granted recipients two alternatives: to conspire in tax evasion, or to be damaged by viruses.

In the case of conspiracy in tax evasion, the senders always provide valid contact methods to induce the recipients to participate in illegitimate activities. These offers seemingly aim to establish a relationship between service provider and clients. Nevertheless, the true effect is that they form a conspiracy. The recipients have to react actively before they become conspirators in tax evasion schemes. The process might involve repeated exchange of e-mail after the initial unsolicited messages. Under these circumstances, the unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information. Thus, the recipients might be less averse to such messages. Such messages become the means of communication for the trespassers and criminals, hence posing great threats to social-control attempts to frustrate illegal activities.

In the case of viruses attack, the senders exploited social engineering to induce recipients to open the messages and subsequently the attachments, by blurring the sender and subject columns and falsifying the message contents and name of the attached files. These messages do not require replies from the recipients before they cause damage. They are also dangerous for the recipients in the sense that they are harming the recipients’ hardware and software, wasting the labour force, and hindering the business.

Time factors in cybercrime

All offences happen in relation to a certain time. Information systems make a more efficient use of time, either in positive social actions or in negative social actions. A single cybercrime can be completed in a very short time, say, seconds or minutes. The simplest example is to modify or destruct data in a hard disk. The more complicated example is the possibility of transferring the U. K.'s total currency reserve in 15 minutes to another country (Kelly 2002). General cybercriminal offences can involve tremendous information transmission in a relevantly short period. For example, in R. v. Kirkwood ([2005] EWCA Crim 3534, 21 December 2005), the accused downloaded 934 computer games and uploaded 592 over a period of three months through his bulletin board, which had specialized in exchanging copyright games.

However, preparation for some kinds of cybercrime may be time-consuming, usually taking several days, weeks or even months. It depends on the attacks projected, the complexity of the process, and the security technology of the targeted users. The more sophisticated the perpetration is, the more time is needed for preparation and processing. The more sophisticated the security measures are, the more time is needed for overcoming them.

Many offences are committed in a particular natural time or social time. Natural time is the time-span depending on the natural cycle, for example, four seasons and 12 months of a year, seven days of a week, twenty-four hours of a day, day and night, etc. Social time is the time span depending on the social cycle, for example, work time and spare time, holidays, etc. Circumstances are particular time-spans accompanied by natural events, such as wind, snow, rain, etc., or social events, such as war, riot, strike, demonstration, etc.

In the traditional crime of bank robbery, robbers have generally to act when the bank is open, when money is in the safe, when money is being transferred by special vehicles. It is not a prerequisite for cybercrime to depend so much on time. In principle, electronic cash can be "stolen or robbed" at any time, whether it is work time or not.

Many traditional offences are environmentally or weather dependent. In the case of cybercrimes, the environment and weather become less important. For example, in traditional larceny, when a thief walks in rainy weather, the footprint may soon be eliminated by water, but the footprint may be left if it is in the snow; the wind may

conceal the sound of a footstep, and it may be more difficult to see the thief in the dark than on a clear moonlight night. In the environment of cyberspace, the factor of weather is nearly irrelevant, that is, cybercrimes are an all-weather business. In whatever kind of weather, cybercriminals can sit at a computer and perpetrate whatever kind of activity without fear that victims or the third parties will discover him in person.

Cybercrime can cross time-zones, so that the “time” in a day, measured by the criterion of law enforcement, is not so relevant in the offence. Traditional offences may be committed in different periods of the day, for example, stealing when it is dark, burglarizing when the house-owner is at work, etc. Online illegal obtaining of information and money may not be time-limited. However, due to strict supervision and the monitoring of online activities, the perpetrators may have to avoid the work time.

Once successful, attacks may continue for a long time, for instance, for several weeks or for several months. In the case of pure illegal access and the obtaining of information from computers, the victim can hardly find the intrusion in the subsequent months. The intrusion may be repeated before the loopholes are fixed. In addition, influences of some kind of viruses on whole information systems may last for several years. Once created, viruses can never be annihilated and prevented from spreading. Although old viruses may become less harmful due to the use of anti-virus, the less protected computers can still be infected in subsequent years. Another example of continuing cybercrime is the Nigerian 419 fraud, which has been prevalent for several decades and is still a big threat to Internet users.

Malicious programmes, frauds and some other cybercriminal tricks, once they have emerged, may be analogous to natural viruses or bacteria. They exist independently despite people’s use of anti-viruses, which are like an immunity injection for human bodies. As viruses or bacteria may infect those for whom the injection has failed to take, the failure of anti-viruses may reveal the vulnerability of the systems. The attack happens wherever there is a security loophole.

Spatial factors in cybercrime

Like traditional crimes, cybercrimes are also more or less related to the factor of

space. The possibility of the trans-territoriality of individual cases is high.

The phenomenon of cybercrime is distributed everywhere. In some cases, offences are committed in such a way that the activities take place in a distributed manner. In R. v. Dooley ([2005] EWCA Crim 3093, 1 November 2005), the court found that such file sharing networks as KazaA could facilitate Internet users to share various kinds of files through changing computers connected to the Internet into servers that were accessible to other members, who then install the same software in their own computers, regardless of the location of the computers.

The frequencies of these cases are different in various regions and countries. The objective description of the global situation proves that though cybercrime is characterized by its universality, it is undeniable that cybercrime cases are rare in some countries. For example in Finland, according to Miettinen (1996), from 1980 to the time his study was published, the officially-investigated hacking cases were only 10-15 in number. Although hacking cases involving one or two million dollars of losses also existed, the frequency and severity of the cases were less comparable with cases that happened in countries such as the U. S. In West European countries, cybercrime is also less serious than in the East European transition countries.

Definitely, cybercrimes also leave some kind of traces in digital form and can be used as clues for a traceback. However, we find that cybercriminals are less anxious about traces of this kind than about the risks of being exposed in person. The straightforward example is a person who will dare to intrude into a computer in a neighbouring room through the LAN, but not dare to enter the neighbouring room without permission to gaze at the computer screen, not to mention operating that computer without permission. If a remote intrusion is in question, such as an unauthorized access from Europe to a computer in the U. S., the user has hardly any fear of being exposed or caught. Therefore, trans-national cybercriminals are less discouraged from engaging in these activities by the deterrence of law enforcement.

The technological nature of cybercrime

In the new millennium, the information economy is a popular expression used by entrepreneurs, while cybercrime is a popular expression used about the criminals. Many scholars have recognized the intensified technological involvement in

cybercrime (For example Conly 1991; Clark and Diliberto 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006). In all cybercrimes, computers and the Internet are used as tools. Even if what is in question is an attack where computers or networks, or information is targeted, the necessary tools are still computers and the Internet, without which the offence may fall into the traditional offences, and cannot be classified as cybercrimes. However, technological involvement is a necessary but not sufficient condition. Illegally assembling computers with market traded computer parts can hardly be a cybercrime. Yet, illegally manufacturing computer chips can be. Definitely, if traditional forces and technological means are combined in a certain offence, both cybercrime and traditional offence can run together. For example, a bank employee may be abducted and forced to reveal the IDs and passwords. The combined use of these means is not rare in practice.

Certainly, the computer may not be the only tool in a certain cybercrime. For example, wireless networks and mobile networks provide particularly complicated ways of making a command to launch an attack.

The extent of technological involvement is different in various cybercrimes, from simply cracking a less complex password to controlling thousands of bots all over the world to launch distributed denial of service attacks. The situation is, regardless of whether straightforward or sophisticated techniques or instruments are used in illegal activities, the damage can always be substantial. Although the overall losses of computer misuse are difficult to calculate, the losses of a single victim may be overwhelming, particularly when an individual does not keep separate back-ups. An attack, even by a straightforward technique, can also result in serious consequences in considering the various detailed situations of victims.

In cybercrimes, in addition to the possibility of manoeuvring multiple computers, the available tools, means and functions are also numerous. In fact, much malicious software can be downloaded from the Internet. Many hacking techniques can be learned online. There are opportunities to purchase a malicious programme from the Internet as well.

The complexity of cybercriminal activities

The Internet allows for the communicating and planning of criminal activities in more different ways than in even the recent past (Lenk 1997, pp. 126-135). The Internet also accommodates exchange of cybercrime methods free of charge, or provides sales of malicious programmes (Behar 1997, p. 66). Advanced criminal mechanisms enable the attackers to avoid prosecution or complicate investigations in a straightforward manner (Sofaer and co-workers 2000). This further enhances their universality and concealment, making law enforcement more and more impossible.

Furthermore, imagine the time when there were only 20,000 computers connected to the Internet globally, Stoll (1988) described the process to trace the break-ins by a persistent computer intruder attacking Lawrence Berkeley Laboratory (LBL). The traceback took nearly a year of work apart from requiring the cooperation of many organizations including the U. S. FBI and the German Federal Criminal Police Office, during which the intruders continued their activities against 450 computers and successfully gained access to more than thirty (Stoll 1988, pp. 484-497). Even then because of the complexity of the cyber environment, investigation of cybercrime cases was extremely time-consuming. Since then, for example, the case of Sean Galvez shows a worsening of the situation. He obtained unauthorized access to 40 eBay customer accounts and incurred up to 32,000 dollars of fraudulent charges in 2003 could only be indicted in 2006 (The Office of the Massachusetts Attorney General, Boston Teen Indicted on Charges He Hacked into eBay Accounts and Stole Victims' Identities, 5 January 2006. Retrieved 14 January 2009, from http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1576). In comparison with cases affecting thousands or millions of computers, the difficulties in investigating these relatively trivial cases poses the question of how the prosecution of a major case is possible.

Johnson (2006, p. 6) has discussed a digital forensic evidence on both national and international levels, the challenge posed by offences of online pornography, encrypted illegal materials, cyber terrorism, cybercrimes against children, and the exploitation of computer viruses in extortion schemes. He found that the process of searching digital documents was extraordinarily difficult, due to the capacity of rapid transmission, storage in remote machines, encryption, or the use of other concealment methods. In 2002 BCSC 524 (In the Matter of s. 490(3) of the Criminal Code and In the Matter of Edmond Edward Edmond et al. 2002 BCSC 524), the Supreme Court of British Columbia found that 102 gigabytes of data had been recovered through the

forensic imaging of computer hard drives, which meant that the printouts of such a volume of data could fill a 12,500 foot high stack of paper. As a result, the work in reviewing the data was time-consuming, and required co-operation from authorities in the United States, Singapore, and Great Britain (paragraph 12). In R. v. Harlos (2005 ABPC 118), the police seized from the offender six hard drives containing storage of 920 gigabytes of data, mostly child pornography: totally 3162 photographic images, and 763 videos of child pornography (paragraph 15).

The Internet being a vulnerable infrastructure, all the individual and institutional Internet users are exposed to similar threats of becoming victims of cybercrime. In practice, as I pointed out in Section 5, all cybercrimes are more or less committed through technological means. Malicious programmes and anti-viruses are "weapons" in information systems. Malicious programmes are usually designed and disseminated without rewards, being uncommercialized and unsystematic. Anti-viruses are designed and sold as commodities. Both of them are products of labour, but with a different use: the former being offensive weapons, the latter being defensive weapons.

McAfee (2005, pp. 2-13) has summarized tools and their functions in cybercrime. These tools are used not only to access confidential information, but also to conceal traces, and prevent normal functioning. Most of these tools can be downloaded from the Internet free of charge or at inexpensive prices. It is especially easy to search and obtain such a programme from the Internet as freeware or shareware using a search engine. Many tutorials are furthermore prepared for non-professionals to study them systematically from primary level.

Compared with malicious programmes, the sources of preventive programmes are fewer in number and more expensive on the market. To search such a programme on the Internet turns out to be more difficult than obtaining are free of charge. The usual results are that the links are redirected to a trial version with limited functions or a full version with payment instructions. The incentives for not revealing such programmes are profits, compared with the incentives for causing broader and larger damage and gaining fame by the revelation of malicious programmes. These cases are akin to cases of copyrights and their infringement.

Both factors, discussed in Sections 5 and 6, can be simplified because of the abundant opportunities for abuse of information systems. In fact, many practical cases have shown that rather than depending on sophisticated technologies and

overcoming complicated processes, the perpetrators simply exploit the opportunities at hand. In Yearly v. Crown Prosecution Service ([1997] EWHC Admin 308 21st March, 1997), the accused, a computer engineer, accessed without authorization a security document in the computer he worked on for a store and he then put it on the Internet. Although his computer knowledge was a condition of his employment, nevertheless, in obtaining the confidential file, opportunity was the most significant element rather than his knowledge and skills. With a malicious intent, everyone with the least knowledge of computer systems but are given the same opportunity would be able to do the same. An offence primarily engenders by opportunity, should not be measured by the sophistication of techniques and the complexity of the processes involved.

The costs of cybercrime

Although much literature dealing with "the costs of crime" has been written by economists, statisticians, jurists, and sociologists, the practical estimate of the costs of one single offence or the whole criminal phenomenon has proved impossible to work out. However, the costs of crime can roughly include direct and indirect costs, physical and psychological costs, and both the costs before the incident and after the incident. There have been efforts to quantify the losses of computer crime, for example Wasik (1991, pp. 34-41), or measuring the size of the problem, for example, Grabosky (2000, pp. 8-9). In respect of the losses caused by cybercrime, it is overall so expensive that no other criminal activity can compare with it. Sometimes, the "losses" of one offence may not necessarily be a pure social cost. Some of the wealth may be transferred from the victim to the offender. Generally, the more the offender obtains physically, the more the victim loses. In some other cases where the offender does not acquire substantial property, mere "losses" of a victim's money or health satisfy the offender's psychological needs. In both cases, the offender has expected benefits. Again, the more the victim loses or the more seriously the victim is hurt, the more the offender is satisfied psychologically (see generally Section 6.7).

Monetary losses caused by crimes, particularly by cybercrimes, are thus difficult to calculate. Direct measurements being unavailable, only some important references can be used to indicate the extent of these losses.

As a first reference, because individuals and businesses have to invest heavily in information security and have to change their behaviour to reduce the probability of being victimized (Gray 1979, p. 13), spending on cybersecurity services and products constitutes, for example, a significant part of the losses brought about by the threats of cybercrime. Without cybercrime, The ICT industries do not require to invest specifically in security protection. In the meanwhile, investment on security protection does not increase productivity. Presently, this expense becomes a necessary part of their ordinary inputs.

The second reference is that losses in individual cases provide a more direct impression. Daler and co-workers (1989, p. 22) reported that the average loss obtaining in a cybercrime case is around 400,000 dollars, as compared with the average take in an old-fashioned bank robbery of 6,000 dollars. The CCIPS web site publishes a list of cybercrime cases prosecuted in the U. S. in recent years. It is obvious that once the cases involve losses, the amount will be large (definitely, there are also cases not involving any monetary loss) (CCIPS 2006). Calculating the 115 cases prosecuted during March 1998 through to May 2006, the lowest single loss was 5,000 dollars, and the highest was 80 million dollars. The average loss in these cases was 1.27 million dollars (Li 2006). The losses involved in single cases differ from each other. The media, for example, reported that the infamous Love Bug of 2000, for example, infected at least 45 million computers and caused losses of millions of dollars (BBC News, 4 May 2000. Retrieved 14 January 2009, from http://news.bbc.co.uk/hi/english/uk/newsid_736000/736570.stm).

The third reference can be obtained from various cybercrime surveys, each of which provides some information about the situation of the respondents. For example, the annually operated CSI (2005) survey on 700 US computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities, found that the reported average financial losses resulting from security breaches are 204,000 dollars per respondent. The total losses for 639 survey respondents came to exactly over 130 million dollars (CSI 2005).

Accurately calculating the losses of cybercriminal offences is a task of some sophistication (UNCJIN 1999, Paragraph 27). Cybercrime is a comparatively easy business, but the deterrence, in its turn, is far from easy. Notwithstanding the fact that the whole world is actively combating cybercrime, the number of cybercrimes is still on the rise and their costs are increasing exponentially (CSI 2000). In 2002, the

estimation of cybercrime losses averaged about 50 billion dollars annually (Hale 2002, pp. 5-6). In 2005, another estimation of losses reached 400 billion dollars (McAfee 2005, p. 5). The meaning of this number from the year 2005 may be well understood if we compare it with the 9/11 attacks that cost New York City at least 17 billion dollars. Further, it may be pointed out that the forecast for the effect of terrorism in general, is a reduction of 0.25 percent of the world economy's growth rate -an impact of around 75 billion dollars (Davidson 2003). If such comparisons are used in measurements, worldwide overall cybercrimes is bleeding the economy of nearly 24 times the sum of the 9/11 attack losses. In addition, companies are investing heavily in a variety of security technologies and insurance (Sofaer and Goodman 2001, p. 5). This is not unrealistic, if we recall that the International Monetary Fund June 2002 Global Financial Stability Report reflects, in a conservative estimate, the total insured losses for 9/11 of around 44 billion dollars (IMF 2002, p. 38).

Besides the direct cost, Loeb has estimated that breaches of confidence can make companies lose more than 5 percent of their market value on average (Loeb 2004, p. 69). A survey by Telang and Wattal (2005) analysed the economic impact on 18 software suppliers and found that announcing vulnerability in one of these companies' products caused a 0.6 percent fall in its stock price, or an 860 million dollars fall in the company's value (Telang and Wattal 2005, p. 3).

Immeasurable are the losses of confidential information on state security, governmental reputation and diplomatic relationships. In McKinnon v USA & Anor ([2007] EWHC 762 (Admin), 03 April 2007), the accused obtained control over dozens of computers belonging to and used by the U. S. Government, through which he could gain further control over hundreds of thousands of computers. Among them were 53 Army computers, 26 Navy computers, 16 NASA computers, and 1 Department of Defense computer (ibid., paragraph 3). Upon gaining access, the accused deleted critical operating systems from some computers, and copied files into his own computer from some other, including passwords, causing a total of 700,000 dollars of loss (ibid., paragraphs 4 and 6). Given there was no further loss from his unauthorized access, the U. S. government has been striving to extradite him for prosecution. The visible and invisible losses made the government unwilling to give up the lengthy proceedings in the U. K., even though his conviction can provide no more compensation for the losses.

In general, what makes the situation worse is not only that cybercrime is expensive, but also that the costs are rapidly increasing. Only if it reaches saturation point, can the speed of development become stable or commence to decrease. Furthermore, in the "competition" between the criminals and law enforcement, it is obvious that the former are more efficient in obtaining new technologies than the latter (Centre for Strategic and International Studies 1998).

The above analysis concentrates on the general impact of cybercrime on society. A special issue requiring clarification is that of the impact of cybercrime on individual victims, comparing a pensioner and a millionaire both of whom are undergoing 100 euros of losses in a cash card fraud. The direct suffering of the former is definitely far more severe than that of the latter. Criminal justice, equally protecting the poor and the wealthy, may reasonably be considered inefficient in equally treating every euro value of property belonging to every person. In addition, traditional crime can be lethal to natural persons, but has a less severe threat to legal persons in general. However, more and more businesses have considered cybercrime more likely to happen (IBM. IBM Survey: Consumers Think Cybercrime Now Three Times More Likely than Physical crime: Changing Nature of Crime Leads to Significant Behaviour-Changes, 25 January 2006. Retrieved 14 January 2009, from http://www-03.ibm.com/press/us/en/pressrelease/19154.wss), and more harmful than physical crimes (IBM. U. S. Businesses: Cost of Cybercrime Overtakes Physical crime: IBM Survey Shows Changing Nature of Crime Causes Organizations to Look Inside, 14 March 2006. Retrieved 14 January 2009, from http://www-03.ibm.com/press/us/en/pressrelease/19367.wss). This is a natural result of increasing importance of information for enterprises and increasing threats of cybercrime to information security.

The following sections (8, 9 and 10) will deal with the issue of "the dark figure" of cybercrime. Traditionally, the dark figure has been formed as a consequence of the criminals' self-concealment, family relationship and even from community reasons (Radzinowicz and King 1977, pp. 31-34). With regard to cybercrime, besides conventional concealment methods, information systems constitute another significant mask for perpetrators, a shelter for the criminal, and a tool for hiding traces.

The anonymity of the perpetrators of cybercrime

Communicating anonymously is a great characteristic of the Internet environment. In using the Internet, anonymity can be kept from the beginning to the end. First, anonymous access to the Internet poses the most serious threat. In many countries, one of the most important forms of using the Internet is realized through cyber cafés or libraries, where anonymous users can access many of the online services. Definitely, there exist different situations in different countries. Compared with Finland where there are few cyber cafés in towns and cities, the cyber cafés in China have become the "third space" of school-aged juveniles besides home and school. The facilities and services in academic or public libraries are far less convenient for users than those in cyber cafés managed by private firms. An increasing number of hacking cases involving the Internet or Internet users are committed or conspired in cyber cafés.

Secondly, anonymous subscription to the Internet services raises the difficulty of identifying users. The personal information provided for the registration of an e-mail account, the name and address of e-mail messages, and the authors' information in Usenet, etc., can all be fabricated. Keeping identity anonymous is favourable for the protection of users from victimization, but it also favours the hiding of perpetrators from being traced.

Thirdly, users can keep their identity anonymous in the process of online communications. There are also mechanisms for keeping complete anonymity by which one user can send messages to other users, and then the messages are transmitted to the final target, such as newsgroup, e-mail list, or a single e-mail account. What makes it more complex is that in the mechanisms the intermediary can only be a programme and may be in another jurisdiction (Kingdon 1994). This also reminds us that there exists the possibility of numerous transmitting points, by which messages are transmitted from one terminal to the next terminal, from that to the next in line, and so on, until the message reached the destination.

Tracing this transmitting process is theoretically possible. During the tracing process, the investigation is exactly the contrary to the process of transmission. Each time, the investigator can trace back one point.

It is likely that all points are identifiable. Nevertheless, as long as there is an unexpected element at any point, the tracing chain can be disrupted without reaching

the original source. According to National Police Agency of Japan (1998), the possible examples include that the victim has no record of the Internet Protocol (IP) address; ISPs do not keep suitable records; hackers alter the logs; or some points are located in countries that have not criminalized hacking. As Koch (2000) has pointed out, theories about detection remain theories, and they are too new to be tested in practice. Even if all the work of traceback is fulfilled, the actual value of this work may be discounted in a judicial process because of different locations and thus diversified jurisdictions.

Fourthly, the specific service or software can play further roles in hiding users. Cybercriminals usually establish anonymizers, which are systems particularly designed to invalidate technical identification of the source of communications (See Belgium's answer to the "Questionnaire 5: Have you received any reports from your law-enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?" in Council of the European Union, Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Brussels, 20 November 2002). In fact, this kind of service or software can also be conveniently obtained free of charge or at an inexpensive price from the Internet. Everyone who is online can get access to these tools and services. Such software is likely to be replicated and spread unlimitedly, creating a bigger population of hidden users who potentially threaten the security of information systems.

Although the anonymity of cybercriminals poses a series of questions, it is still the core of the "perfect environment" for the criminals (Levinson 2002, p. 455, saying that anonymity is exploited by perpetrators of old crimes such as fraud, pornography, gambling, stalking and identity theft, or new crimes such as unauthorized access, denial of service, and malicious programmes, pp. 455-458); yet it is at the same time welcomed by Internet users. People are constantly concerned that without online anonymity, it could be impossible to guarantee fundamental rights (COM(2000) 890 final, p. 20; National Police Agency of Japan 1998). It is not strange that the European Union Data Protection Working Party's Recommendation recognized that online anonymity brings about a dilemma for governments and international organizations (The Article 29 Data Protection Working Party 2001): in particular, in maintaining human rights to privacy and freedom of expression, and combating cybercrimes (COM(2000) 890 final, p. 20). Philip (2002) warned that

anonymity can provide users with “the courage to do the outrageous and sometimes even resort to illegal activities.”

Hidden victims: underreporting and unwilling to report

Cybercriminals have a greater advantage than most of the traditional criminals in respect of the low probability of arrest and conviction. Many scholars have mentioned this characteristic of cybercrime, as noted in the literature cited in this section. Hatcher and co-workers (1997, pp. 397, 399) have pointed out that many cybercrimes are not reported. The term “dark figure”, used by criminologists to refer to unreported or unrecorded crime (As Radzinowicz and King (1977) pointed out that, “The recorded figures of crime are huge but the reality behind them everywhere looms far larger. The sinister word dunkelziffer (dark figure) was coined at the turn of the century to express this hidden reality.” See Radzinowicz and King 1977, p. 42), has been applied to denote undiscovered cybercrimes (UNCJIN 1999, Paragraph 30). Many intrusions are not detected for a variety of reasons (COM (2000) 890 final, p. 11). Cybercrimes can well be described as hidden crimes (Cook (1997) used “hidden crimes” to denote under-reported or under-recorded crimes such as domestic violence, sexual assault, and racial harassment (p. 55-58). He also used “hidden victims” to denote the victims of the “hidden crimes” p. 127).

At the same time, victims of cybercrime are willing to be hidden victims (Cook 1997, p. 127). The usual “motives for silence” concerning victimization may fall into one of the following categories: 1. The idea that the victimization is not worth the mobilization of justice; 2. Involvement; 3. Pressures of fear; 4. The uneasy accessibility of police and court; and 5. The ignorance of events by the police (Radzinowicz and King 1977, pp. 38-40).

In sketching the victim decision-making, Greenberg and Ruback (1985) have established a three-stage model: the victim judges whether the event is a crime, evaluates its seriousness and decides what to do (Greenberg and Ruback 1985, as cited by Feldman 1993, p. 26). Before these stages, one stage that is more important should be added, that is, whether the victim knows the event. If this is the case, the reporting of cybercrime may remain at a lower level, because cybercrime is invisible and difficult to discover; it is more difficult for the victim to judge whether the event

is a crime and to estimate the losses; and the victim has less knowledge about whether there is an agency to report the crime. The limited reporting of the cybercrime has been noted more than 20 years ago by Parker and Nycum (1984, p. 313), who studied the invisibility of computer crime. At present, the Internet's virtual environment has made the situation still worse. Fortunate progress in proving material evidences in traditional crimes was made in late 1980s when DNA tests were first introduced (Levinson 2002, p. 537). However, digital evidence in computer crimes are immune from such high-technological testing measures. The invisibility of cybercrimes is based on several factors, either technological or human (UNCJIN 1999, Paragraphs 30, 31). Sometimes, the simple reason is that the victims are not willing to report, or even do not know where to report the case (Salgado 2001). The documented reasons for the reluctance to take legal actions are mainly fear of adverse publicity, public embarrassment or loss of goodwill, loss of investor or public confidence, resulting economic consequences such as the panic effect that this information would create on their stock prices (See Carter 1995, p. 21; Roush 1995, pp. 32, 34; Gelbstein and Kamal 2002, p. 2; McKenna 2003), and exposure to future attacks (COM (2000) 890 final, p. 11). The UN suggested that these factors have a significant impact on the detection of cybercrime (UNCJIN 1999, Paragraph 31).

Yet there are other reasons for the victim to keep silence. While many people are active in maintaining their interests and rights, some people view victimization as their own failure in life and career and are not willing to reveal the fact of their failure to any individuals and institutions, so as not to make public their own weakness.

Therefore, it is inevitable that the rate of unknown instances of cybercrimes has increased as a result. The CSI (2005, p. 20) summarized the reasons why the U. S. organizations did not report intrusions to law-enforcement agencies in 2005, including unawareness of law-enforcement interest, a civil remedy seeming the best course, computer would use to their advantage, and negative publicity would hurt the image of their stock. This survey has indicated the percentages of respondents identifying each stated reason as being very important in their decision not to report computer intrusion. At the same time, it is worth noting that the reasons are subject to changes in each annual survey.

The concealment of cybercrime traces

Mitchell and Banker (1997, pp. 707-711) have concluded that there are four characteristics in which cybercrimes are different from traditional crimes, that is to say, difficulties in detection, limited reporting, jurisdictional complexities, and resource constraint. All these four aspects fall under the broad characteristic of concealment. The concealment of cybercrimes has been brought about by other technological and human factors (Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006).

Most of traditional offences are highly visible due to apparent depredations, presence of witnesses, and so on. There are also traditional crimes that occur in private places and become less visible (Walsh 1983, p. 236). Unlike traditional threats where criminals are physically present at the crime scene, cybercriminals are usually not present at the crime scene thus making apprehension difficult (Speer 2000, p. 260). In information systems, executing a command to delete files does not mean that the files are permanently deleted. What happens is merely that files are hidden due to a change in file names so that the files can be recovered, except when a secure-eraser programme is in use (See for example, International Airport Centres, L. L. C., et al v. Jacob Citrin (Seventh Circuit No. 05-1522, 24 October 2005, p. 2). Skilful criminals can disable this kind of security mechanism, and conceal the data that might possible be taken as evidence in prosecution.

Technological advances have both a positive impact on businesses and a negative impact on law enforcement (Institute for Security Technology Studies 2002). For example, in the DrinkOrDie case, the online software piracy group concealed its actions by various security measures: exchanging e-mails via private mail server using encryption; using a nickname to identify members, and communicating about group business only in closed, invite-only IRC channels; the FTP sites, where tens of thousands of pirated software, game, movie, and music titles were deposited, were secured by particular authentication mechanisms (U. S. Department of Justice, Press release, 17 May 2002). On the other hand, the available technological solutions have not completely met the requirement of data collection, log analysis, and Internet protocol tracing (American Society for Industrial Security 2004, p. 40). There is also the necessity for law-enforcement agencies to recruit personnel with "electrical engineering and computer-science backgrounds" (Fields

2004, p. B1);

Inevitably, critics point out that cyber police have extra incentives than combating cybercrime, for example, asking for more money, more wiretap, bugs in computers and sell phones, weak encryption and permission to implement security technology, without more arrest following (Koch 2000).

Concealment of crimes has important economic effects. Stanley (1995, p. 2) stated that concealment of crime can decrease the incentives not to perpetrate, and increase the costs of law enforcement. Concealment of cybercrime demonstrates the low probability of punishment. In the U. S., only one in 100 cases was detected, one in 8 prosecuted, while only one in 33 prosecuted cybercrimes resulted in a prison sentence. That is to say, the likelihood that a cybercriminal would be put into prison was a one in 26,400 chance (Daler and co-workers 1989, p. 22), as compared with the likelihood of imprisonment in traditional bank robbery a one in three chance (ibid.). Law-enforcement agencies found that a majority of cybercrimes never reached the criminal-justice system. Even in the relatively few cases where a crime was reported, most often the criminal's identity was never discovered (Phrack magazine, Identifying Net Criminals Difficult, volume 18, number 53, 8 July 1998, article 14, 0X1. Retrieved 14 January 2009, from http://www.phrack.org/phrack/53/P53-14). As a consequence, as Radzinowicz and King (1977, p. 67) pointed out, “The calculation of chance is as applicable to the commission of crime as to many other activities.” Given other factors constant, if cybercrime is more concealed than other offences, the potential perpetrators are more motivated to take illegal actions on the Internet, and thus more offenders of traditional crime will be prepared to migrate to cyberspace.

The trans-territoriality of cybercrime coverage

Free flow of information from one country to another is a goal of information systems (Directive 95/46/EC, Preamble (3); UN A/RES/51/162; Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 12), but trans-border flow is not free. The trans-border information flux is accompanied by risks of crime of a similar nature. In any country, the court must have jurisdiction over the person or the subject-matter of a lawsuit. This works well with the current set-up of law-enforcement agencies that are

territorial and are operating in different villages, towns, districts, cities, counties, states or provinces, or national boundaries. Nevertheless, unauthorized access to information systems can be accomplished from virtually anywhere on the networks, because the communications capability of cyberspace allows criminals to conspire more easily, without geographical proximity to one another or to the target (Lenk 1997, pp. 126-135). The international characteristic of cybercrime is evident (National Police Agency 1998). In fact, some of the cases prosecuted have been of this nature, for instance, R. v. Kozun (2007 MBPC 7), where the forensic analysis of the computer of the accused disclosed that 165 separate users from 15 countries had traded through his computer. The computer was converted into an automated trading centre through a programme, by which 141 users had traded in the previous 13 days.

The sphere of legal jurisdiction makes the cybercrime enforcement more complicated (Lee and co-workers 1999, p. 873). Smith, Grabosky, and Urbas (2004) concluded that the trans-national dimension of cybercrime posed four formidable challenges for prosecutors, who have to determine whether the conduct in question is criminal in their own jurisdiction, collect sufficient evidence to mobilize the law, identify the perpetrator, and determine his or her location, and decide whether to leave the matter to the local authorities or to extradite the offender (Smith, Grabosky and Urbas 2004, pp. 48-49).

Sinrod and Reilly (2000, p. 2) have pointed out that although some international organizations are examining cooperative mechanisms in the field of fighting against cybercrime, many of their members are slow in recognizing the urgency of the situation.

The elimination of borders favours inter-jurisdictional mobility of crime. Due to the actual difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way can easily lead to punishment. Reasonably, suggestions have been made to incorporate cyberspace into various jurisdictional frameworks. Nonetheless, this needs a great deal of time, agreement, and co-operation between countries, which are still struggling to take common actions.

Finally, it is worth noting that trans-national cases only constitute a minor part of cybercrime (Li 2006). No certain conclusion can be drawn because it is possible that trans-national offences are not as prevalent as scholars have assumed. On the other hand, it is difficult to reveal these offences for reasons that scholars have laid bare. Or, it may be, that it is simply law enforcement does not put sufficient emphasis

on these offences. Before credible data are available to give an answer to this question, we have certain reasons to claim that trans-national offences have sometimes of a dual nature: they do not appear as prevalent as domestic offences, but they are more difficult to detect and convict. In addition, because the investigation of trans-national offences is more expensive and time-consuming, law enforcement will not give more priorities to these offences than to cases that have happened “close to home”.

The rampancy of cybercriminal phenomena

On the computer age, Bequai (1978, p. 4) said, the computer was a gigantic calculator enabling people to gain large quantity of data by pressing a button. When the computers are connected as a colossal network, “buttons” are used not only to acquire and transmit data, but also to replace some of the traditional interpersonal communications and social interactions. Collin (1999) explained the sense of the virtual world, being “symbolic - true, false, binary, metaphoric representations of information - that place in which computer programmes function and data moves.” Cyberspace has developed into a stockroom of the wealth and power of the information age (London School of Economics and Political Science 2001). The pervasive application of ICT can be regarded as a magnitude change of the contemporary society. It poses new challenges to the traditional conception and system from many aspects, and it changes the routine activities of a large population of the members of society. This change, among other effects, will benefit the disorganization of the traditional social structure and thus increase the presence of motivated perpetrators and the exposure of their victims. As a phenomenon long existing in society, crime has transformed its forms and grown steadily in different historical periods. Criminal phenomena have always gone beyond the law. New forms of crime will inevitably emerge from a continually developing society, while the law is not ready to guard against them. The requirement for punishing crime requires a revision of criminal legislation and a renovation of criminal justice. The persistent extension of the ranges of crime can but result in the constant extension of the regulating domain of criminal law.

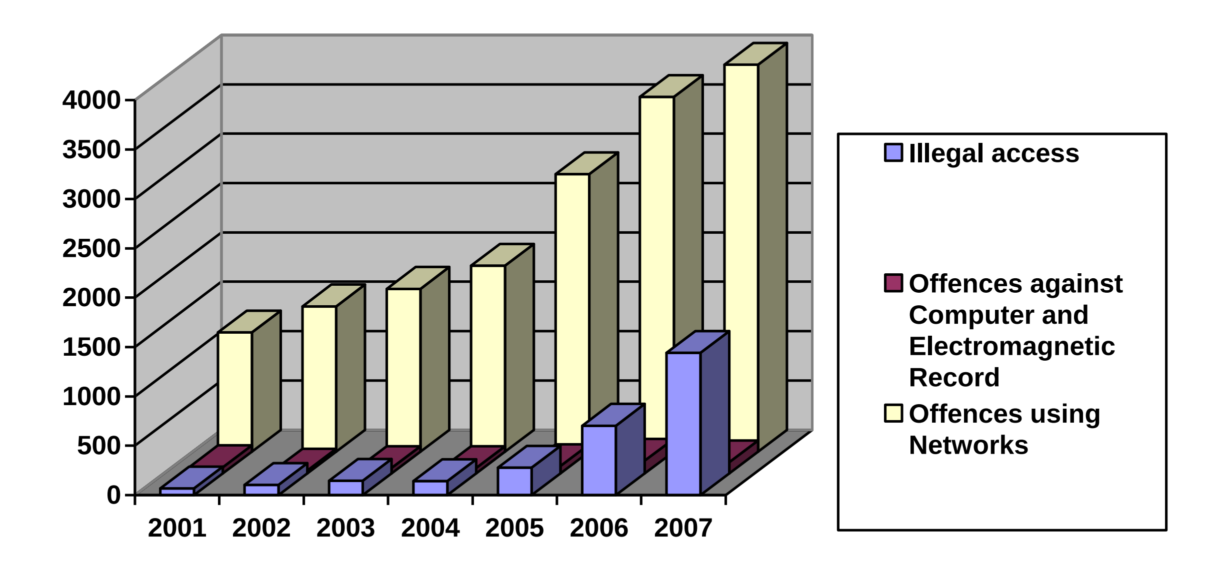
People longed for the industrial society in which their economic situation would

be improved, the education level enhanced, consciousness civilized and traditional crime decreased. However, not only has traditional crime not decreased, but also white-collar crime came into being. Where white-collar crime was the offspring of an industrialized civilization, cybercrime concomitantly grew in hand with an informationized civilization. The unprecedented combination of crime and computer creates a stage of anti-productivity, undermining the magnificent prospects for high technology. Criminals abuse the conditions of the emerging market and technologies.

The rise and prevalence of the Internet has become the prominent intervention factor in the development of cybercrime in the recent decade. On the Internet, exist universal contradiction and contention, use and abuse, defence and offence, ethic and deviance, fact and falsification, order and disorder. The powerful software and hardware that enable people to work more effectively is difficult to operate securely (Allen 2001, p. 2). Speedy technological evolution makes the vendors concentrate more of their time on the market, and less time on security features (Pethia 2001). Although computers and networks are at present protected by various means, the emerging vulnerabilities are inevitably increasing.

All these considerations concerning criminal phenomena in the background of high-technology development does not imply that it is the technology that brings about more crimes. Nevertheless, we cannot deny the factor that the adoption of the new technology may make the crimes more profitable, and less risky (Daler and co-workers 1989, p. 21). Even worse, the criminal will tend to repeat his or her criminal acts-- especially when there is little chance of being caught or convicted. Consequently, cybercrime would pave the safest way to illegal profit, considering the ease with which it can be committed and the negligible chances of imprisonment (Daler and co-workers 1989, p. 21).

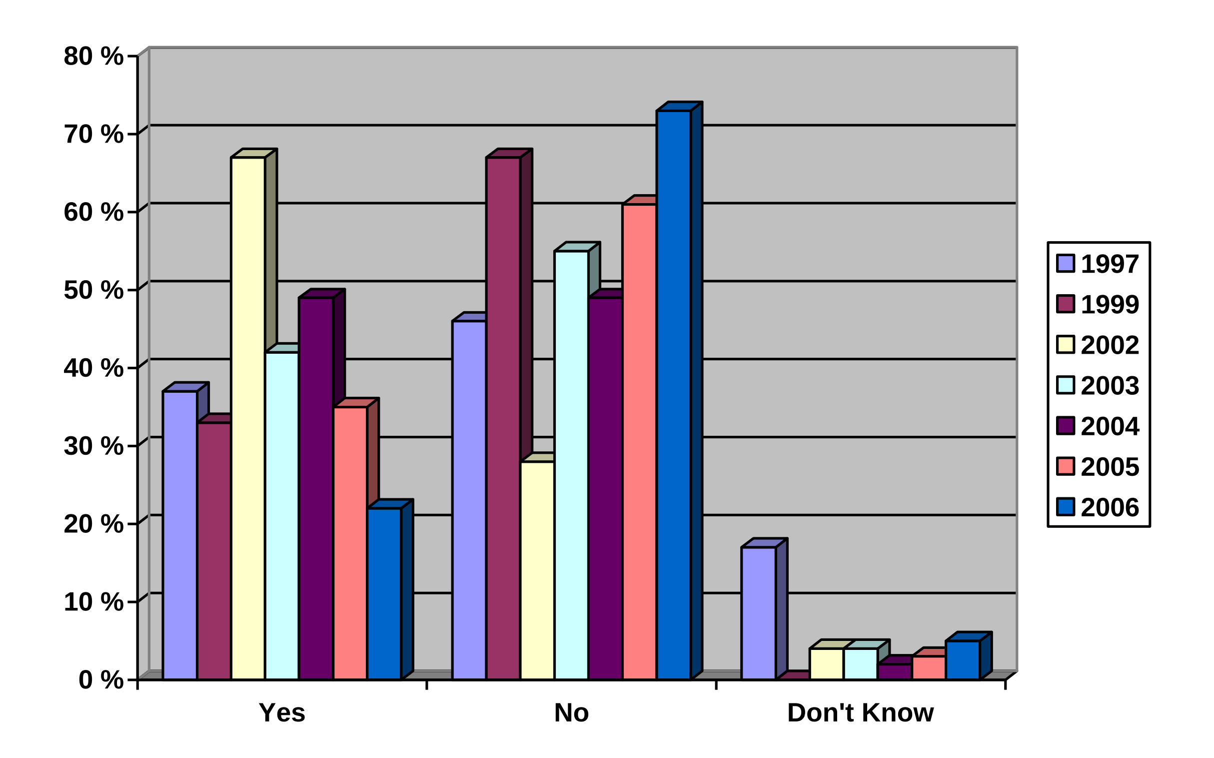
Even under these circumstances, arrests for cybercrimes are statistically growing, just to take Japan as an example. There, the total number of arrests of cybercriminals increased from 913 in 2000 to 3,918 in 2007, while it reached 2,192 in the first half of 2008 (National Police Agency 2008).



Illustrated according to the statistics of the Japan National Police Agency, Concerning the Situation of Arrests and Consultancy of Cybercrime in 2006, 22 February 2007; the Japan National Police Agency, Concerning the Situation of Arrests and Consultancy of Cybercrime in 2007, 29 February 2008.

Figure 21 Arrests for Cybercrime in Japan in the Past Six Years

The findings of the cyber security and cybercrime survey are another way of viewing the situation. Australia and the U. S. have carried out annual survey for years. In Australia, the ferment years when the organizations surveyed experienced incidents or attacks against their information systems were 2001, 2002, and 2003 (the answers in Figure 26 were given one year later).



The above figure is based on the statistics from the Australian Computer Crime and Security Survey, collected in 1997, 1999, and during 2002-2006 annually. The figure presents the answer to the question "Did your organization experience computer security incidents or attacks against its computer systems in the last 12 months?" This figure refers to the following reports, even though in each report the results of several years' survey are usually included:

Australian Computer Emergency Response Team 2002, p. 5; 2003, p. 11; 2004, p. 12; 2005, p. 13; 2006, p. 17.

Figure 22 Security Incident Trends in Australia

In the U. S., the zenith years of cybercrime were 1997 to 2002 (see Figure 27, the answers were indicators of the situation of the year previous). Both Australia and the U.S. show a fall in positive answers, but the victimization rates are still high. In Australia, it is around 20 percent. In the U. S., it is around 50 percent. In criminological language, they show a victimization rate of 20,000 and 50,000 per 100,000 populations.

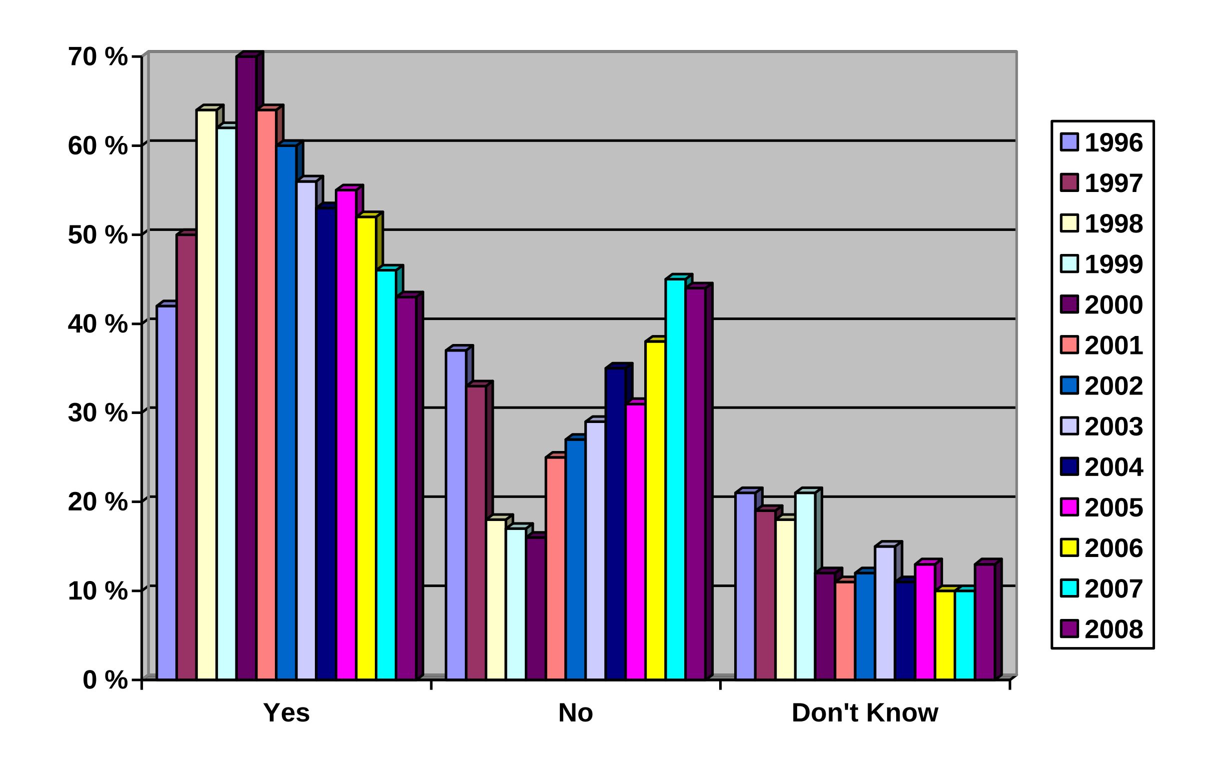


Figure 23 Unauthorized Use of Computer Systems in the USA

The above figure is based on the statistics in the reports on CSI/FBI Computer Crime and Security Survey done annually. The figure illustrates the trends concerning the "unauthorized use of computer systems within the last 12 months" in the USA over the past 13 years.

The figure refers to the following reports, even though in each report the results of several years' survey are usually included: CSI 2000, p. 8; 2001, p. 4; 2002, p. 6; 2003, p. 6; 2004, p. 8; 2005, p. 11; 2006, p. 10; 2007, p. 10; 2008, p. 13.

Rent-seeking from the exaggeration of insecurity

The social reaction to and impression on cybercrime are broadly diversified. The general public who are not unfortunate enough to experience or witness real life offences usually rely on the reports of the mass media. While the mass media have their own interests other than maintaining a peaceful and secure daily life, the texts, graphics, audio and video files they compose and create can distort criminal incidents. Some characteristic ways of reporting computer crime have been misleading, even though they play roles in reinforcing the public consciousness of security (Molnar 1987, p. 714). In observing the social reaction to crime, Felson

(2002) coined the term “dramatic fallacy” as one of his “ten fallacies about crime” (These ten fallacies about crime comprise a dramatic fallacy, a cops-and-courts fallacy, a not-me fallacy, an innocent-young fallacy, an ingenuity fallacy, an organized-crime fallacy, a juvenile-gang fallacy, a welfare-state fallacy, an agenda fallacy and a whatever-you-think fallacy. See Felson 2002, pp. 1-18): media have interests in seeking strange and violent incidents to keep their ratings high, in which process a highly inaccurate general picture of crime is painted (p. 1).

The tendency to dramaticize and mystify offences that the general public do not often hear about and see stems from the benefits gained by the mass media from their show-off through selective reports. They choose to broadcast what they consider capable of attracting an audience, while at the same time they keep a silence about events in which they have less interest. The most important principle of the media is to be authentic. However, their authenticity is built on selective reports. First identified by Gordon Tullock (1967), rent-seeking finds its way into cyberspace. Anderson (2001) has contributed to the study of exaggeration of cyber insecurity by pointing out in his paper that many interest groups would unavoidably engage in manoeuvring the truth of the cyber insecurity to benefit from the scared market.

The players may include the mass media, the security engineering community, security professionals, police officers and even professors (Anderson 2001). Schneier (2004, pp.87-89) has criticized the fact that software vendors may have an incentive to exaggerate insecurity. In fact, Hoo (2005, pp. 67-69) has suggested that straightforward, cheap measures are much more worthwhile than large projects that many security vendors prefer to sell. There is definitely a problem that many organizational users leave their computers on and online the whole night after work, many without complex access control. Broadband networks provide a convenience for individual and organization users to keep online 24 hours a day, and seven days a week (Traditional networks are through dial-up connections. Now, two methods of broadband service are digital subscriber line (DSL) and cable modem service. Fiber optics, etc. are gaining ground. See Earthlink Inc. vs. FCC, District of Columbia Circuit No. 05-1087, 15 August 2006). Sometimes those who are their contacts can even find their online status in the chat or e-mail systems. The 24-hour-online model is practically more risky than a dial-up service in terms of longer online time.

Doing this research, I have found that many manufacturers of computer hardware and software also have a tendency to provide a darker picture to users when

presenting the problem of cybersecurity. This becomes easier to understand when we recall that these manufacturers are striving to survive the growing threats of consumers' awareness against the market of their products. In order not to subject them to product liability, they have to adopt a preparatory stance of impressing the users and judicial organs that the reason for cyber attacks lies not in the defects of their products but in the malicious motives of the perpetrators.

While many people are motivated to exaggerate the truth, Harvey (Financial Times, 3 December 2003) has claimed that cyber terrorism remains an insignificant issue in real life. Evidence can be seen from the detailed documents such as "A Chronology of International Terrorism for 2004", in which none of the incidents that caused deaths and injuries have employed or targeted computers and networks (National Counterterrorism Centre 2005). In fact, if we consider the urban-crime problem in the U. S., as Miethe (1995, p. 15) did, more than one-fourth of the households were victimized by crime in 1992, while one-half of the population would be victimized by a violent crime in their lifetime. The natural reaction is that cybercrime remains a less than prevalent fear. Although what Wasik (1991, p. 150) suggested that in the future information systems can be used in cases such as murder and injury, the traditional "direct-contact predatory crime predominates" in present society (Felson 2002, p. 23). Apparently, however, the people who are currently engaged in various security services may more easily grasp the more powerful mass media coverage than the traditional offences. The Internet as a part of the mass media airing news about a new computer virus is far more spectacular than what traditional newspapers, radios or TV programme can do about a theft, fraud or murder. By all accounts, most of the current popular knowledge about cybercrime comes from the mass media, regardless of the degree of reliability of such sources.

Cybercrime as a business[2]

In many cases, various cybercrimes are committed as a profitable business. One of the most significant examples is spyware. The traditional notion of spy has multifaceted meanings. Spies can always be classified into positive spies, neutral spies and negative spies, based on their roles for or against classifier's interests according to classifier's judgment. Undoubtedly, spy being good or bad are dependent

---

[2] This section is adapted from my article "Spyware, Spy Affairs, and Anti-Spy Actions," to be published.

on who spies and for whom the spy spies. With spyware's purpose for develop and target for operation, spyware can be regarded as having been developed as a new business. Unlike original types of malicious software that was created solely for the purpose of destroying users' hardware, software, or data, subsequent variants of malicious software have increasingly meddled in users' control over their own machines and data. When new variants evolved from their malicious software ancestors, they nurtured the new ambition for seeking profits. Many different players are participating in the division of labor and share of profits in this business. These players can be divided into two categories: insiders and outsiders.

Inside players are those who make a profit on or take a loss from being positively or passively involved in spyware-related activities. They can further be divided into three subcategories:

A. Symbiotic inside player: producer, beneficiary, and victimized target user. Core players in spyware industry are they, whose activities are necessary components in the industry, and without whom the emergence, existence and development of the industry would be impossible.

B. Autoecious inside player: victimized target user protector. They are those who claim to be representatives of consumers and other users. Their just existence has been dependent on the reality that consumer rights are frequently infringed.

C. Successive inside player: anti-spyware industry, security expert, legislator, law enforcement. They are those who seek overall solutions against spyware. Nevertheless, their opportunities rely on the emergence and existence of negative influence of spyware.

Outside players are those who make use of the existence of the reality of spyware-related activities. They can further be divided into three subcategories as well:

A. Symbiotic outside player: non-beneficiary and non-victim observer. They those who are indifferent to the occurrence of spyware phenomena and the actualization of spying.

B. Autoecious outside player: mass media. They are those who claim to disclose actual facts behind the phenomena of spyware. Yet they do not take strict scientific approaches in their investigation.

C. Successive outside player: researcher and teacher. They are those who describe the phenomena, reveal the reality, explore the impact, explain the discovery, discuss different ideas, reason the hypothesis, and establish a theoretical frame.

These players have different attitude towards the creation, dissemination, operation, mischief, and general prevalence of spyware: many of them can benefit from the just negative effect of spyware on users, networks, and society (see Table 15).

Table 15 Attitude of Involved Players in Spyware Business

	Spyware tolerance	Spyware neutral	Spyware averse
Creator	Sense of achievement, financial gain, earning a high reputation		
Customer	Exploiting the function of spyware to advertise, spy and attack opponent		
Target user	Fulfilling customization, getting advertised, etc.	Nothing special happens, enjoying some small annoyances	Being exploited of time, concentration, energy, and psychic. Hardware being slowed down, network being disconnected, personal information being stolen
Intruder	Easy to control others		
Real spy	Easy to spy others		
Advertiser	Easy to inform others of its products or services		
Hardware manufacturer	Encouraged to invent securer and faster machine, and new and good machine makes more money. If Microsoft Windows Vista can run on an Intel Pentium 100 machine, then many current computer companies will bankrupt.		

Hardware vendor			Old types of machine may be excluded by slowing-down brought about by spyware. Hardware vendor may have a little bit to lose.
Updated hardware vendor	New type of hardware has broader market		
Software writer	Encouraged to write more secure software		
Software vendor			Old software may be disqualified in the new security environment. Anyway, software vendor has little to lose.
Updated software vendor	New software has broader market		
Anti-spyware producer	Winning market through panic created by spyware's broad spread. Whenever there is spyware and other viruses, there is a market for anti-virus producer. All viruses of bad nature are welcome. If you don't scare users, then we will be dismissed.		
Security expert	Current experts enjoy higher reputation and status, and get more employment opportunities		Current security expert may feel too busy dealing with security problems, and have to learn more sophisticated skills.
Mass media	Job opportunities, and new headlines		
Legislator	Job opportunities		
Law enforcement	Job opportunities, and new reason for budget		More work load, and new skill requirement
Professor	New field of academic career		
Researcher	New field of academic career, project and new funding opportunities		

Under such circumstances, numerous strong players in the field of spyware are motivated by one and the same goal: profit. Then the weak players will entirely have no way go get rid of the destiny of being victimized. What makes it more defenseless is that, other offences committed online can correspondingly be operated as a business, the scale of criminality and victimization will thus be expected to expand incessantly.

Conclusion

According to the basic conclusions of the last sections, we have identified a number of factors that complicate the reporting, detection, investigation, prosecution, conviction, and sentencing of cybercrime. People call for making the punishment fit the cybercrime (Vamosi 2003). However, practicable methods of enhancing law enforcement have not been at hand.

The development of cybercrime necessitates a timely update of the law, as some countries have done. However, it seems that the laws implemented are inadequate for effectively addressing the problem (Vamosi 2003). An example of this aspect can be found in the definition of fraud in U. K. The traditional fraud definition required that a person but not a computer be deceived (Daler and co-workers 1989, p. 125). Thus, the application of fraud provisions has depended on whether a *person* has also been deceived. These authors have mentioned that only in other countries, not the U.K. have the provisions on fraud been interpreted more broadly.

According to the McConnell International (2000, pp. 3-6), only 31 percent of the countries surveyed had substantially or fully updated their laws, 15 percent partially updated, while more than half of the countries had no updated laws. According to the principle of legality, the absence of a law punishing cybercrime sets the deterrent probability at zero, while the actual punishment is also zero. This being the situation, the expected utility of the offender equals the utility when he or she is undetected. By recognizing this benefit, the potential perpetrators will have a greater incentive to commit cybercrime than other offences.

As the conclusions of McConnell International (2000, p. 8) have demonstrated, light punishments create limited deterrence. The possible reason why creating a virus carries lighter penalties than marijuana offences (McCullagh 2004) may be due to the

elasticity of these two kinds of crime from the economists' point of view. Unlike the marijuana offences that are inelastic, cybercrime is more elastic. Tougher punishment for drug crime will be less effective than for cybercrime. However, considering the marginal deterrence when the effect of punishment is too weak to stop cybercrime, this definitely does not deter, either. Lack of a certain degree of severity in punishment will not prevent potential criminals from committing the crimes they are planning, because even if they are probably caught, their expected benefit will still be higher than the expected cost. It is the marginal deterrence of the punishment but not the elasticity of the crime that is working.

However, at the same time, methods adopted in some countries cannot be completely explained by the above theory. Take the example of the application of long-term imprisonment for offences with a low detection probability. The expenses of the long-term imprisonment are quite huge. Thus, it may be said that under these circumstances, governmental investment is insufficient when the emphasis is put on punishment, and detection is ignored. This relates to the value orientation of the government.

Some other countries completely violate the principle of rational choice. They seem to find it difficult to afford adequate funding for detection, conviction, and enforcing punishment, while on the other hand they have established a cyber police, employing huge police forces. The tasks of these cyber police include detection and evidence collection, as well as cybercrime prevention with techniques and human resources, forming a "cyber information dam". The expense is also huge. As Dnes (2000, p. 75) pointed out, it is of very poor value to increase the probability of conviction through employing more police officiers.

In these countries, the concerns about the privacy of individuals have to give way to national security and the maintenance of social order. This means that in the information age, the public organs receive ever greater powers of surveillance and interception. Since the 1990s, the terrorists have frequently launched attacks; and individualism is gradually being submerged by the voice of national interests and international co-operation. The role of punishment in the deterrence of crime is undoubtedly unearthed. Whether in poor or wealthy countries, severe punishment is being used universally for cybercrime. This can be explained as decreasing the expected benefits of cybercrime while increasing the expected costs, forcing the offenders to give up committing the offences and to select instead legal activities.

This implies that the means the modern countries take to decrease crime are direct prevention, plus increasing detection probability and increasing punishment severity.

Nevertheless, the following factors deserve further consideration. First, it remains a doubtful question as to whether the information dam can effectively control the information flood. The filtering and blocking of information is expensive and ineffective. As a substitute for severe punishment, it is either a necessary waste of democracy (compared with over-criminalization), or a necessary limit to democracy (compared with information freedom). In order for cybersecurity to be maintained, the private sectors and the public authorities should cooperate to strengthen the legal frameworks for cybersecurity (McConnell International 2000, pp. 8-9).

Secondly, a surer answer can be provided to the question of whether severe punishment is cheap. There have been hundreds of studies done concerning the cost of the death penalty, proving that the death sentence is expensive as well as being easy to execute the innocent. These have become common-sense reasons for repealing the death penalty. The cost of imprisonment is also high. Because the cost of severe punishment is costed differently in different countries, the legislature and law enforcement have a different tendency in implementing various degrees of severity in implementing punishments, which can bring about further jurisdictional problems.

Finally, what should be researched is whether severe punishment is effective. Given that the probability of detection remains extraordinarily low, and that there is no appropriate approach to increase it, a severe punishment again runs up against a limitation. A severe punishment to some extent requires the support of the probability of detection. If not, it loses the basis on which it exists and delivers little deterrence at all.

Cybercrime differs from traditional crimes in its universality, anonymity, concealment, and complexities. While quantitative evaluation of cybercrime has proved difficult, the fight against cybercrime has become a big burden for companies. Because of difficulties in detection, investigation, and conviction, the dark figure of cybercrime remains high. The harsher penalties should be applied to pursue effective deterrence, but in themselves they do not serve protection.

In effect, we are still repeating Radzinowicz and King's dilemma (1977): the perpetrator may escape detection, the detected perpetrator may escape arrest, the arrested perpetrator may not be brought to book due to lack of evidence, the

perpetrator brought to book may be released because his innocent context or trivial offence, the prosecuted perpetrator may escape conviction, and the convicted perpetrator may only be imposed a light penalty (p. 41).

The themes explored in this paper show that there is no easy way of bringing cybercriminals before the judicial process. Nevertheless, the increase of cybercrime is constant, and the reinforcement of deterrence is a constant need, yet for these two forces to reach equilibrium is still an on-going process.

References

Allen, J. 2001. CERT System and Network Security Practices, in *Proceedings of Fifth National Colloquium for Information Systems Security Education*, George Mason University, Fairfax, Virginia, 22-24 May. Retrieved 14 January 2009, from http://www.theebusinesssite.com/PPT/SecureWebsites-769468/769498_Reading_Class8-CERT_Network_Hardening.pdf

American Society for Industrial Security (ASIS). 2004. Cybercrime-Fighting Tools Still Lacking, *Security Management*, number 40.

Anderson, R. 2001. Why Information Security Is Hard--an Economic Perspective, in *Proceedings of the 17th Annual Computer Security Applications Conference*, Washington, DC: IEEE Computer Society. Retrieved 14 January 2009, from http://www.acsac.org/2001/papers/110.pdf

Australian Computer Emergency Response Team. 2002. *2002 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2003. *2003 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2004. *2004 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2005. *2005 Australian Computer Crime and Security Survey.*

Australian Computer Emergency Response Team. 2006. *2006 Australian Computer Crime and Security Survey*.

Behar, R. 1997. Who's Reading Your E-mail? *Fortune*, number 66, pp. 57-70.

Bequai, A. 1978. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books.

Carter, D. L. 1995. Computer Crime Categories, *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation, volume 64, number 7, pp. 21-26.

CCIPS. 2006. Computer Intrusion Cases. Retrieved 14 January 2009, from http://www.usdoj.gov/criminal/cybercrime/cccases.html

Centre for Strategic and International Studies (CSIS). 1998. *Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo (CSIS Task Force Report)*, Centre for Strategic and International Studies.

Clark, F. and Diliberto, K. 1996. *Investigating Computer Crime*, Boca Raton, Florida: CRC Press LLC, 1996.

Collin, B. C. 1999. The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, *11th Annual International Symposium Criminal Justice Issues*. Retrieved 14 January 2009, from http://www.crime-research.org/library/Cyberter.htm

Commission of the European Communities. 2000. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*, COM (2000) 890 final.

Conly, Catherine H. 1991. *Organizing for Computer Crime Investigation and Prosecution*, Darby, PA: Diane Publishing.

Cook, Dee. 1997. *Poverty, Crime and Punishment*, London: CPAG.

CSI. 2000. CSI/FBI 2000 Computer Crime and Security Survey.

CSI. 2001. CSI/FBI 2001 Computer Crime and Security Survey.

CSI. 2002. CSI/FBI 2002 Computer Crime and Security Survey.

CSI. 2003. CSI/FBI 2003 Computer Crime and Security Survey.

CSI. 2004. CSI/FBI 2004 Computer Crime and Security Survey.

CSI. 2005. CSI/FBI 2005 Computer Crime and Security Survey.

CSI. 2005. CSI/FBI 2005 Computer Crime and Security Survey.

CSI. 2006. CSI/FBI 2006 Computer Crime and Security Survey.

CSI. 2007. CSI/FBI 2007 Computer Crime and Security Survey.

CSI. 2008. CSI/FBI 2008 Computer Crime and Security Survey.

Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. 1989. *Security of Information and Data*, Chichester: Ellis Horwood.

Davidson, A. 14 April 2003. Decentralization, Disease and Terrorism. Retrieved 14 January 2009, from

http://www.eclicktick.com/decentralization__disease_and_terrorism__.htm

Dnes, A. W. 2000. The Economics of Crime, in N. G. Fielding, A. Clarke and R. Witt. (eds.). *The Economic Dimensions of Crime*, London: Palgrave, 2000, pp. 70-81.

Dunlop, C and Kling, R. 1991. Introduction to Security and Reliability, in C. Dunlop and R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, San Diego: Academic Press, 1991, pp. 524-532.

Feldman, P. 1993. *The Psychology of Crime*, New York, NY: Cambridge University Press.

Felson, Marcus. 2002. *Crime and Everyday Life*, third edition, Thousand Oaks, California: SAGE Publications.

Fielding, N. G., Clarke, A. and Witt, E. 2000. *The Economic Dimensions of Crime*, London: Palgrave.

Fields, G. 6 April 2004. Cyberexperts and Engineers Wanted by FBI, *Wall Street Journal*, B1.

Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.

Gotterbarn, D. 1990. Computer Ethics: Responsibility Regained, *National Forum: The Phi Kappa Phi Journal*, volume 71, number 3, pp. 26-31. Reprinted in D. G. Johnson and H. Hissenbarn (ed.). *Computer Ethics and Social Value*, Englewood Cliffs, New Jersey: Prentice Hall, 1995, pp. 18-24.

Grabosky, P. 2000. Cyber Crime and Information Warfare, The Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service and held in Canberra, 9-10 March. Retrieved 14 January 2009, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

Gray, C. M. 1979. The Costs of Crime: Review and Overview, in C. M. Gray. (ed.). *The Costs of Crime*, Beverly Hills, CA: SAGE Publications, pp. 13-32.

Greenberg, M. S. and Ruback, R. B. 1985. A Model of Crime Victim Decision Making, *Victimology: An International Journal*, volume 10, pp. 600-616.

Hatcher, M. and co-workers. 1999. Computer Crimes, *American Criminal Law Review*, volume 36.

Hoo, J. S. 2000. How Much is Enough? A Risk Management Approach to

Computer Security, *Centre for International Security and Cooperation Working Paper*. Retrieved 14 January 2009, from http://iis-db.stanford.edu/pubs/11900/soohoo.pdf

Institute for Security Technology Studies (ISTS). 2002. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment*.

International Monetary Fund (IMF). 2002. *Global Financial Stability Report, A Quarterly on Market Developments and Issues*, International Monetary Fund.

Johnson, D. G. 1985. *Computer Ethics*, Englewood Cliffs: New Jersey: Prentice Hall.

Johnson, Thomas A. 2006. *Forensic Computer Crime Investigation*, Boca Raton, Florida: Taylor and Francis Group.

Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 14 January 2009, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime

Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 14 January 2009, from http://www.catalaw.com/logic/docs/jk-isps.htm

Koch, L. Z. 10 July 2000. Open Sources Preventing Cybercrime, *Inter@ctive Week*.

Lee, M. and co-workers. 1999. Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, *Berkeley Technological Law Journal*, volume 14, number 2, pp. 839-885.

Lenk, K. 1997. *The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing, The Governance of Cyberspace*, Routledge, New York, 126-135.

Levinson, D. (ed.). 2002. *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.

Li, X. 1993. Jisuanji Fanzui Ruogan Wenti zhi Yanjiu (*A Study on Several Issues of Computer Crime)*, degree thesis for Master of Laws, China University of Political Science and Law.

Li, X. 2006. The Criminal Phenomenon on the Internet, *University of Ottawa Technology and Law Journal*, vol. 3, no. 2 (in press).

Loeb, M. P. 1 April 2004. The True Cost of Cybercrime, *Network Computing*.

London School of Economics and Political Science. 2001. Cybercrime: the

Challenge to Leviathan?. Retrieved 14 January 2009, from http://www.lse.ac.uk/clubs/hayek/Essays/cybercrime.htm

Mandia, Kevin and Prosise, Chris. 2003. *Incident Response and Computer Forensics*, Emeryville, California: McGraw-Hill/Osborne.

McAfee. 2005. *Virtual Criminology Report: North American Study into Organized Crime and the Internet*.

McConnell International. 2000. Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. Retrieved 14 January 2009, from http://www.witsa.org/papers/McConnell-cybercrime.pdf.

McCullagh, D. 19 August 2004. Punishment Fails to Fit the Cybercrime, *ZDNet United Kingdom*. Retrieved 14 January 2009, from http://www.crime-research.org/news/19.08.2004/574/

McKenna, B. 2003. United Kingdom Police Promise Charter to Guard Good Names, *Computers and Security*, volume 22, number 1, pp. 38-40.

Miethe, T. D. 1995. Fear and Withdrawal from Urban Life, in Wesley G. Skogan, ed. *Reactions to Crime and Violence*, Thousand Oaks, London, New Delhi: SAGE Periodicals Press, pp. 14-27.

Miettinen, J. E. 1996. *Survey of Hacking in Finland in the 1990s- Summary of the Results*, Oulu: University of Oulu.

Mitchell, S. D., and Banker, E. A. 1998. Private Intrusion Response, *Harvard Journal of Law and Technology*, volume 11, number 3, pp. 699-732.

Mohay, G., Byron, C., Vel, O., McKemmish R., and Anderson, A. 2003. *Computer and Intrusion Forensics*, Norwood, Massachusetts: Artech House.

Molnar, J. 1987. Putting Computer-related Crime in Perspective, *Journal of Policy Analysis and Management*, volume 6, number 4, Privatization: Theory and Practice, pp. 714-716.

NPA. 1998. *The Situation of High-tech Crime and the Suppression of Police, Japan Police White Paper*, Tokyo: National Police Agency.

NPA. 1998. *The Situation of High-tech Crime and the Suppression of Police, Japan Police White Paper*, Tokyo: National Police Agency.

NPA. 2008. *Concerning the Situation of Arrests and Consultancy of Cybercrime in the First Half of 2008*, 21 August, Tokyo: National Police Agency.

Nycum, S. H. 1983. Testimony on Computer Security before the U. S. Senate Subcommittee on Oversight of Government Management of the Committee on

Governmental Affairs, *Computers and Society*, volume 13, number 4 and volume 14, Nos. 1, 2, and 3.

Parker, D. B. 1980. Computer Abuse Research Update, *Computer/Law Journal*, vol. II, no. 2, pp. 329-352.

Parker, D. B., and Nycum, S. H. 1984. Computer Crime, *Communication of the ACM*, volume 27, number 4, pp. 313-315.

Pethia, R. D. 2001. Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks? Before the House Committee on Government Reform,

Philip, A. R. *The Legal System and Ethics in Information Security*, SANS Institute, 2002. Retrieved 14 January 2009, from http://www.securitydocs.com/go/1604

Pihlajamäki, Antti. 2004. *Tietojenkäsittelyrauhan rikosoikeudellinen suoja: datarikoksia koskeva sääntely Suomen rikoslaissa* (The Protection of Data Processing under Criminal Law: Provisions on Data Crimes in the Finnish Criminal Code), Helsinki: Suomalainen lakimiesyhdistys.

Radzinowicz, L. and King, J. 1977. *The Growth of Crime: The International Experience*, London: Hamish Hamilton.

Roush, W. 1995. Hackers: Taking a Bite Out of Computer Crime, *Technology Review*.

Salgado, R. P. 2001. Working with Victims of Computer Network Hacks, *USA Bulletin*, volume 49, number 2.

Schneier, B. 2004. Hacking the Business Climate for Network Security, *Computer*, volume 37, number 4, pp. 87-89.

Sieber, U. 1998. *Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission*. Retrieved 14 January 2009, from http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

Sinrod, E. J., and Reilly, W. P. 2000. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, volume 16, pp. 177-232.

Smith, George. 8 September 1998. Truth is the First Casualty of Cyberwar, *Wall Street Journal*.

Smith, Russell G., Grabosky, Peter and Urbas, Gregor. 2004. *Cyber Criminals on Trial*, Cambridge: The Press Syndicate of the University of Cambridge.

Sofaer, A. D. and co-workers. 2000. *A Proposal for an International Convention*

on Cyber Crime and Terrorism, Centre for International Security and Cooperation.

Solarz, Artur. 1981. *Computer Technology and Computer Crime*, Stockholm, Sweden: Research and Development Division.

Speer, D. L. 2000. Redefining Borders: The Challenges of Cybercrime, *Crime, Law and Social Change*, volume 34, pp. 259-273.

Stanley, T. J. 1995. Optimal Penalties for Concealment of Crime, *Economics Working Paper Archive*.

Stephenson, Peter. 2000. *Investigating Computer-Related Crime*, Boca Raton: Florida: CRC Press LLC.

Sterling, Bruce. 1994. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Austin, Texas: Electronic Release. Retrieved 14 January 2009, from http://www.gutenberg.org/dirs/etext94/hack12.txt

Stoll, C. 1988. Stalking the Wily Hacker, *Communication of the ACM*, volume 31, number 5, 484-497. Reprinted in C. Dunlop and R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, San Diego: Academic Press, 1991, pp. 524-532.

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, 26 September. Retrieved 14 January 2009, from http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html

Tavani, H. T. 2000. Defining the Boundaries of Computer Crime: Piracy, Break-ins, and Sabotage in Cyberspace, *Computers and Society*, volume 30, number 4, pp. 3-9.

Telang, R, and Wattel, S. 2005. Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis, Presented at *the Fourth Workshop on Economics and Information Security, Boston*, 1-3 June.

Thompson, D. 1989. Police Powers - Where’s the Evidence? *Proceedings of The Australian Computer Abuse Inaugural Conference*.

Tullock, G. 1967. The Welfare Costs of Tariffs, Monopolies and Theft, *Western Economic Journal*, volume 5, pp. 224-232.

UNCJIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, nos. 43 and 44.

Vacca, John R. 2005. *Computer Forensic: Computer Crime Scene Investigation*, Hingham, Massachusetts: Charles River Media.

Vamosi, R. 10 September 2003. Make the Punishment Fit the Cybercrime, *CNET Reviews*. Retrieved 14 January 2009, from http://reviews.cnet.com/4520-3513_7-5073597-1.html

Walsh, D. P. 1983. Visibility, in Dermot Walsh and Adrian Poole (eds), *A Dictionary of Criminology*, London, Boston, Melbourne and Henley: Routledge and Kegan Paul.

Wasik, Martin. 1991. *Crime and the Computer*, Oxford: Clarendon Press.

Chapter VII Domestic Platform for Social Order in Cyberspace: the Case of China

Abstract

This article provides a study on the criminalisation of cybercrime and control over the Internet in China. In order to exercise control over the Internet, China took a series of actions characterized by criminalization of cybercrime, content filtering and activity monitoring, in order to maintain the state stability as well as cybersecurity. The recruitment of cyber police, the investment on security technology, the requirements on the Internet enterprises, and the surveillance on the users, form a close net to prevent cybercrime.

Keywords: Cybercrime, criminality, criminalization, control over the Internet, China

Introduction to the background of cybercrime in China

The mid-1990s witnessed the advancement of information and telecommunications technology with a faster speed than ever before. Information systems have got individuals, businesses and governments all over the world connected. The increasing convenience for the creation, deposit, processing, transmission, and retrieval of information improves the quality of social life on the one hand, brings about relevant risks and threats on the other.

It is not strange that people consider information systems in China as employed as a modern instrument in an ancient territory (Sunergy Beijing 1997). The challenge that many countries are confronted with in the advent of the information age, that is, how to benefit from the pervasive use of information systems while avoiding a negative political and legal impact from uncensored information, is also eroding the footstone of the Chinese Great Wall. Furthermore, the migration of the criminal phenomenon into information systems-facilitated cyberspace has attracted increasing attention due to its high speed of expansion. The Penal Law of China (1997) provides the fundamental criteria and guidelines for convicting and sentencing cybercrime.

With the assistance of with a series of other laws and regulations, a legal system is being formed to suppress the spread of the so-called new century's pestilence in the cyberspace. People around the world doubt that the explosion of new and pertinent statutory laws over the past two decades reflects society's attempts to wrestle with an ancient phenomenon in a modern context. It remains unknown whether the current approaches to deter and redress cybercrime will prove successful.

This article will analyze the situation of cybercrime, the legislation on cybercrime and punishment, and the policy of preventing cybercrime through control over Internet in China. The article will also analyze the subject, the means, the mechanism and the main purpose of control over Internet, with empirical review of its actual effects and defects.

Situation of cybercrime in China

The mid-1980s symbolised an unprecedented change of China. The development and application of information and communications technology was integrated into the bigger programmes of scientific and technological modernisation (Dai 2003, p. 9). Concurrently, the first computer offences took place in China also in this period (Li 1992). The banking systems became the earliest victims from which money was embezzled, misappropriated and defrauded. In this period, the forms of computer crimes were simple, mainly perpetrated against property; especially those committed in one's duty. In the meantime, the number of the cases was small, while the harm of the cybercrime was great. Therefore, these unprecedented cases evoked wide social repercussions.

Central issues drawing public attentions was on one occasion focused on computer viruses, because the "Ping-Pong" virus, the first virus that sneaked into the Chinese boundary via technical route, caused great panic among the computer users. From the viewpoint of the expensiveness of the computer and the importance of the system, the harmfulness of the computer crime was considerably critical. In computers with slow central processing units and small cache memories, viruses exhausted the system resources, slowed down the operation and destruction and deleted data. Creating and spreading computer viruses was an important form of computer crime. The difficulty in investigation made the detection rate extremely low. At the time, computer viruses have broken down some stock exchanges and

supermarkets in China. However, until 1989 when viruses of political propaganda emerged, the Chinese government began to realize that computer crime was really a “crime” but not a “game”. Even at present, viruses still pose a serious computer security problem for the country.

A new stage of cybercrime began from 1996 with the open access of Internet to general users. The China’s economy has been developing rapidly in the recent thirty years, creating a growing demand for newer and better information technology. China participates in the construction of a global information infrastructure. The computer networks, however, was developed somewhat late in China. In 1987, the first electronic mail from China to the outside world was sent. In 1994, China joined the global Internet. In 1996, the Internet became commercially available. This made clear that China realized the disadvantages of being left behind, and made the great attempt to keep up with the global changing environment. At the time, approximately 15,000 Chinese were online. The 1996 witnessed a four-fold increase in the number of service providers and a ten-fold increase in the number of subscribers. According to China Internet Network Information Centre (2006), China had around 20 Internet Service Providers (ISP) and almost 100,000 users. After ten years, the China Internet Network Information Centre reported that the Internet users in China grew to 111 million users by 2006 (p. 4). The number of network users in China is roughly doubling every one year or two years. These researches clearly indicated the rapid Internet growth in China. Besides, computer hosts 49.50 million (p. 7), domain names registered totalled 2,589,956 (p. 7), and WWW websites 694, 200 (p. 7), total bandwidth of leased international connections 136,106M (p. 9).

With the rapid development of the Internet in China, the cybercrime cases have been increasing: the number of cybercrime cases was approximately 100 in 1998, a 7-fold increase than 1997 (Huasheng Newspaper 1999). In 1999, the investigated cases increased to 400; in 2000, 2,700 cases were opened. In 2001, the cases reached 4,500 (Han and Meng 2004). In 2004, the detected cases totalled 14,000. In 2005, the daily spam averaged 60 million, and 1,800 obscene websites were shut down (Ministry of Public Security 2005). The cases involving the pornography creating, duplicating and spreading are remarkable. The offences against property by the means of networks occupy a majority. The offences against the cybersecurity increase apparently. Computer viruses infection rate remains high. The cases infringing individuals’ rights also increase fast. The cases of threatening the state security continue to increase.

Criminalization of cybercrime

Crimes and criminals come in all varieties on Internet, ranging from the catastrophic to the merely annoying (Icove and co-workers 1995). Therefore, defined broadly, the term “cybercrime” could reasonably include a wide variety of criminal offences, activities, or issues. In China, the term has been the same from the beginning, pronounced as “Jisuanji Fanzui”, that is, computer crime. Now, more frequently used term is “Wangluo Fanzui”, that is, crime on networks. Nevertheless, there has never been an official term for it. The crimes provided in the Penal Law of China are more complicated.

As for the scholars, they introduced a variety of definitions from the Western countries or put forward some new definitions, including the definitions either in the broad sense or in the strict sense. Most of these definitions have been derived from the Western countries, along with the translation into Chinese and publication of books and articles (For example, the definition established in 1979 by the United States Department of Justice, stated that a computer crime is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution). The later study saw some rational thinking about the issue, and some definitions came into being which possess the Chinese style. The definitions introduced to China and proposed by Chinese scholars had profound academic significance before the amendment of the Penal Law in 1997.

Three layers of cybercrime conception

Being a conception with a broad explanation, cybercrime has been defined in China’s laws at three different levels:

At the first level, computer crime is prescribed by Articles 285, 286 and 287 of Penal Law of 1997 in Chapter VI Crimes of Disrupting the Order of Social Administration. According to Penal Law, computer crime is a crime in which computer information systems are the target of crime. A comprehensive definition can be summarized as:

Computer crime is the act of violating state regulations and intruding into computer systems with information concerning state affairs, construction of defence

facilities, and sophisticated science and technology; or violating states regulations and deleting, altering, adding, and interfering in computer information systems, causing abnormal operations of the systems and grave consequences; or violating state regulations and deleting, altering, or adding the data or application programs installed in or processed and transmitted by the computer systems, and causing grave consequences; or deliberately creating and propagating computer virus and other programs, which sabotage the normal operation of the computer system and cause grave consequences (Articles 285, 286 and 287, China Penal Law 1997). Considering the criminalization of cybercrime at this level, the criminalizing scope is too narrow to cover the practical illegal acts related to computer, and necessitated enlargement in the legislation.

At the second level, we can say that the definition of the Penal Law is of only nominal meaning. In fact, cybercrime in China covers quite wide a range. When discussing the problem of cybercrime, we should use the term in the criminological sense but not limited to the Penal Law. As Li (1992) pointed out that, the traditional Penal Law of China can be interpreted and adjusted to punish cybercrime offences with different existing provisions. In fact, it has been the practice in China and many other countries where there were no law dealing with computer crime but computer crimes occurred. The cases that the criminals were detected but not punished were rare. This does not deny that many other cases were left undetected and many detected cases were left unpunished due to substantive and procedural law issues.

At the third level, there are still more academically induced categories. Computer-related crimes can exist in every chapter of the Penal Law, from crimes against the national security to crimes against economy, from crimes against person to crimes against property, etc. (Li 1992) Furthermore, "a sharp distinction between law and policy does not exist in China…policy can have exactly the same effect as formally enacted legislation." (Clarke 1999) This is determined by the methodology of the Chinese mode of thinking, which is on the same basis as the repealed system of guilty analogy.

All of the three levels of meaning of cybercrime are of the same importance when we study the issues of laws, regulations and policy on cybercrime in China. It is necessary to point out that some articles strangely described that "China does not seem to possess any written law or code specifically outlining its computer crime statutes...trials are held by the force of military law..." (Kim 1997) Unfortunately,

there was an apparent misunderstanding on the present Chinese legal system.

The punishment to the crimes differs from fixed-term imprisonment to death penalty, being decided by what kinds of crimes are committed. To punish cybercrime, the Supreme People's Court (2001) ruled that capital punishment might be applied to those who cause provide state secret to foreign individuals or institutions via the networks and cause particularly serious harm.

Detailed survey of criminalization of cybercrime in China

Computer crime emerged in China in mid-1980s and was punished within the previous legal framework. According to Chinese law, computer was only an object or a tool of various crimes. These crimes could cover offence of anti-revolutionary, offence against public security, offence against personal rights and democratic rights, offence against property, offence against social management order, and offence of malfeasance. Different provisions can deal with different situations. The development of the Internet and the offences on the Internet propel the development of the law.

Specific regulation on cybercrime began in 1994 when the State Council promulgated the Ordinance on Security Protection of Computer Information System (Ordinance on Security Protection of Computer Information System, Promulgated by State Council Decree NO. 147, 18 February 1997). The Ordinance prescribed legal liability for the acts of: (1) violating security ranking protection systems of computer information systems, and threatening the computer information systems; (2) violating the registration system of computer information systems international networking; (3) not reporting cases happened in the computer information systems according to the prescribed time; (4) refusing to improve after receive the notice from the public security agency requiring improving the security situation; and (5) other acts threatening the computer information systems (Ordinance on Security Protection of Computer Information System, Chapter 4).

These acts are punishable by public security for admonition or rectification upon stopping the computer (Ibid, Article 20). If the act violates the public security management, it is punishable according to Regulations on Public Security Management; if the act constitutes an offence, it should be held criminally liable according to Penal Law (Ibid, Article 24).

The problems of this provision are two aspects:

In case the act constitutes an offence, it is punishable according to Penal Law.

However, the Penal Law of the time did not provide relevant punishment for any offence involving computer system or computer networks (Penal Law of People's Republic of China, 1979). The provision of "when the act constitutes an offence, it should be held criminally liable" lacked of legal basis.

Another problem was that the subject of liability was not clarified. For example, in the provision of "not reporting cases happened in the computer information systems according to the prescribed time" (Ordinance on Security Protection of Computer Information System, Article 24 (3)) obviously imposed liability to the party of victim. That is to say, the users are both the target of the hacking and the subject of liability.

However, the interpretation function of the Chinese law is so strong that any legal loopholes can be filled through interpreting and applying the existing law. Therefore, hacking is an act punishable according to Penal Law of 1979. Although the provisions in Penal Law of 1979 were very vague, the openness was strong enough to cover new offences. Nevertheless, the disposal of computer crime remained confronted with legal blank.

The amendment of Penal law in 1997 added two articles on computer crimes, that is, illegal intrusion into computer information systems in Article 285 and destruction of computer information systems in Article 286. The Penal Law was promulgated at the beginning of the year, but the Internet developed rapidly just in the same year. The computer crime was prescribed by the Penal Law, but the new problems on the Internet challenged the newly enacted law immediately. In order to react to the new problem, the Standing Committee of the National People's Congress promulgated a comprehensive law to maintain the Internet security in 2000 (The Standing Committee of the National People's Congress, Decision on Maintaining Internet Security, passed on the 19th Plenary Meeting of Ninth Session Standing Committee of the National People's Congress on 28 December 2000). It is the only law on Internet security passed by the legislature, besides Penal law.

(i) Criminalizing intrusion into computer information systems

The offence of intrusion into computer information systems is the act of intrusion into computer information systems of national affairs, national defence construction, and the field of advance science and technology, violating national provision (Penal Law, Article 285). Management Measures of Security Protection of International Networking of Computer Information Networks provides that without

permission, entering the computer information networks or using the computer information network resources is listed as the activities of threatening the computer information networks security and prohibited (Ministry of Public Security, Management Measures of Security Protection of International Networking of Computer Information Networks, ratified by State Council on 11 December 1997, entering into force on 30 December 1997. Article 6 (1)). In provisions regulating the Internet online services business locations, managing units and online users are prohibited from illegal intrusion into computer information systems or destructing function, data and applied programs of computer information systems and threaten the security of information networks (Ordinance on Management of Internet Online Services Business Place, Article 15 (2)). Obviously, these provisions presented the needs of extending the prohibition of hacking activities to what the Article 285 of the Penal Law could not cover, and added the prohibition of using resources of computer information networks without permission. Violating law, administrative regulations, without permission, entering into computer information networks or using resources of computer information networks, should be given warning by the public security agency, those involving illegal income, illegal income should be confiscated, individual or unit should be combined with a certain sum of fine. In case the situation is grave, should be combined with the punishments of interruption of online services and rectification beyond shutting down the computers not longer than six months. If necessary, may propose the previous institutions that granted the certificate or examined and approved withdraw the managing license or abrogate the qualification of online services; if the act constitutes the act violating public security management, punish according to the Ordinance on Public Security Management Sanctions; if the act constitutes offence, imposing penal liability according to the Penal Law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 20).

The Decision on Maintaining Internet Security restated that the act of intrusion into computer information systems of national affairs, construction of national defence, and advanced science and technology that constitutes a crime, should be imposed penal liability according to Penal Law (Decision on Maintaining Internet Security, Article 1 (2)). However, the Decision remains no to punish the general hacking activities, excluding the intrusion into computer information systems not belonging to China, and excluding the computer information systems not belonging

to the above three specific categories.

(ii) Criminalizing content-related offences

The Internet contents posed great challenge to the state security and social stability. The first provisions concerning the Internet contents were implemented in Temporary Provisions on Management of International Networking of Computer Information Networks of 1996 (Temporary Provisions on Management of International Networking of Computer Information Networks, promulgated by State Council Decree No. 195 on 1 February 1996, amended according to "State Council Decision on Amending 'Temporary Provisions on Management of International Networking of Computer Information Networks'" on 20 May 1997). The Provisions require that the units and individuals that are engaged in the Internet business should abide by the related law and administrative regulations, strictly enforce the security and secrecy systems, must not engage in transgress and criminal activities of threatening state security and revealing state secret and other activities with the Internet, must not create, retrieve, duplicate and spread information that disturbs the social security and obscene and erotic and other information (Temporary Provisions on Management of International Networking of Computer Information Networks, Article 13). The Provisions provided that acts violating these provisions, and violating other laws and administrative regulations as well, should be punished according to related laws and administrative regulations; if constituting a crime, should be imposed penal liability according to Penal Law (Ibid., Article 15).

According to China's law, the Provisions presented the determination of Chinese government to punish the criminal activities on the Internet. In the meanwhile, it is obvious that the emphasis of the Provisions was on the control of the Internet contents, and particularly three categories of information related to state security, public security and obscene and erotic information were prohibited. It implied the possibility of punish the activities of creating and spreading computer virus, instructing hacking knowledge as creating and spreading information impeding the public security. More seriously, browsing certain information was also prohibited by these Provisions.

In Management Measures of Security Protection of International Networking of Computer Information Networks, the prohibition on the Internet contents was expanded to nine aspects, primarily covering state security, social stability and personality and reputation, but no reaction to economic interests. The Internet was

firstly regarded as a potential political threat. As for the influence on the economy, it was not considered. The Management Measure prescribed that no unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 5): (1) inciting to resist, breaking the Constitution, laws, or the implementation of administrative regulations; (2) inciting to overthrow the government or the socialist system; (3) inciting division of the country, harming national unification; (4) inciting hatred or discrimination among nationalities or harming the unity of the nationalities; (5) making falsehoods or distorting the truth, spreading rumours, destroying the order of society; (6) promoting feudal superstitions, sexually suggestive material, gambling, violence, murder, terrorism or inciting others to criminal activity; (7) openly insulting other people or distorting the truth to slander people; (8) injuring the reputation of state organs; (9) other activities against the Constitution, laws or administrative regulations.

Since 2000, the prohibitions on the Internet contents were re-combined. However, they remained nine aspects. The most significant change was the adding of the prohibition of "breaching state religious policy, preaching the teachings of evil cults." The prohibition on the Internet contents was further strengthened, with the coverage broadened. In a series of governmental documents afterwards, the new nine prohibitions were specially emphasized. These governmental documents included the Internet services of different departments and different fields. In September 2000, the State Council passed simultaneously the Ordinance on Telecommunications (Ordinance on Telecommunications, passed on 31st Standing Meeting of State Council on 20 September 2000, and promulgated by State Council Decree No. 291 on 25 September 2000) and Management Measures on Internet Information Services (Management Measures on Internet Information Services, passed on 31st Standing Meeting of State Council on 20 September 2000, and promulgated by State Council Decree No. 292 on 25 September 2000). The Ordinance provided that no organization and individual may create, duplicate, publish and spread message containing these contents with the telecommunications networks (Ordinance on Telecommunications, Article 57). The Management Measures provided that the Internet information service provider must not create, duplicate, publish and spread message containing these contents (Management Measures on Internet Information Services, Article 15). Ministry of Information Industry's Management Provisions on Internet Electronic Bulletin Services (Ministry of

Information Industry, Management Provisions on Internet Electronic Bulletin Services, November 2000) provided that no one may publish message containing one of these contents in the electronic bulletin service system (Ibid, Article 9). Ministry of Information Industry's Temporary Provisions on Management of Internet Website Engaged in Business of News Publication (Ministry of Information Industry, Temporary Provisions on Management of Internet Website Engaged in Business of News Publication, November 2000) provided that the news published by Internet website must not contain these contents (Temporary Provisions on Management of Internet Website Engaged in Business of News Publication, Article 13). Ministry of Education' Notice on Printing and Distributing "Management Provisions on Electronic Bulletin Services of Colleges and Universities Computer Networks" (Ministry of Education, Notice on Printing and Distributing "Management Provisions on Electronic Bulletin Services of Colleges and Universities Computer Networks", Jiao She Zheng (2001) No. 10 on 21 October 2001) provided that bulletin board system website users should abide by the provisions by related laws and regulations, and must not create, duplicate, publish and spread messages containing these contents (Management Provisions on Electronic Bulletin Services of Colleges and Universities Computer Networks, Article 13). Management Measures on Internet Domain Names (Ministry of Information Industry, Management Measures on Internet Domain Names, entering into force on 30 September 2002) provided that no organizations or individuals may register and use domain names containing these contents (Management Measures on Internet Domain Names, Article 19).

The new prohibitions cover the following aspects: (1) information that goes against the basic principles set in the constitution; (2) information that endangers national security, divulges state secrets, subverts the government, or undermines national unity; (3) information that is detrimental to the honour and interests of the state; (4) information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity; (5) information that undermines the state's policy towards religions or that preaches the teachings of evil cults or that promotes feudalistic and superstitious beliefs; (6) information that disseminates rumours, disturbs social order, or undermines social stability; (7) information that spreads pornography or other salacious materials; promotes gambling, violence, homicide, or terrorism; or instigates crimes; (8) information that insults or slanders other people, or infringes upon other people's legitimate rights and interests; or (9) other information prohibited

by the law or administrative regulations.

Shortly, some governmental documents concerning the Internet to different extent supplemented the nine new prohibitions. Ten prohibitions appeared. That is to say, a prohibition on “threatening social morality or national excellent cultural tradition”, listed before the previous ninth prohibition. These documents included Ordinance on Management of Internet Online Services Business Place (Ordinance on Management of Internet Online Services Business Place, promulgated by State Council Decree No. 363, entering into force on 15 November 2002), which provided that no management units of Internet online services business place and online consumers may use the Internet online services business place to create, download, duplicate, retrieve, publish, spread or use messages containing these contents by other means (Ordinance on Management of Internet Online Services Business Place, Article 14); Article 17 of the General Office of Press and Publications and Ministry of Information Industry’s Temporary Provisions on Internet Publication Management (Temporary Provisions on Internet Publication Management, entering into force on 1 August 2002) provided that Internet publications must no publish these contents (Temporary Provisions on Internet Publication Management, Article 17); Ministry of Culture’s Temporary Provisions on Internet Culture Management (Temporary Provisions on Internet Culture Management, entering into force on 1 July 2003) provided that Internet culture units must not provide cultural products containing these contents (Ibid, Article 17).

In the General Bureau of State Broadcasting and Television’s Management Measures on Video and Audio Programs Spread on Internet and other Information Networks (General Bureau of State Broadcasting and Television, Management Measures on Video and Audio Programs Spread on Internet and other Information Networks, entering into force on 10 February 2003), the prohibitions were further extended to 12 aspects, adding the false information and overseas programs received and recorded from the networks or overseas media as programs forbidden to spread through information networks (Management Measures on Video and Audio Programs Spread on Internet and other Information Networks, Article 19).

As an important law criminalizing certain activities on the Internet, the prohibitions in the Decision on Maintaining Internet Security can be summarized as three categories nine aspects. The law provided that if any one commits one of these acts and constitutes a crime, should be held liable according to Penal Law. The

prohibitions and applicable Penal Law provisions three aspects:

(1) Maintaining state security and social stability

(a) The acts of exploiting the Internet to disseminate rumours, slander or publish, spread other harmful information, instigate to subvert state regime, overthrow socialist system, or instigate to split the state, undermine the state unity (Decision on Maintaining Internet Security, Article 2 (2)), constitute offence of instigating to subvert state regime (Punishable according to the provisions of Articles 105 (2), 106, 56 and 113 of Penal Law) and offence of instigating to split the state (Punishable according to the provisions of Articles 103 (2), 106, 56 and 113 of Penal Law).

(b) The act of stealing, divulging state secret, intelligence or military secret (Decision on Maintaining Internet Security, Article (2)), may constitute offence of stealing, spying out, purchasing, illegally providing state secret, intelligence (Penal Law, Articles 111, 113, and 56), offence of illegal obtaining of secret (Ibid, Article 282 (1)), offence of illegal possessing of state secret (Ibid, Article 282 (2)), offence of internationally divulging state secret (Ibid, Article 398), offence of negligently divulging state secret (Ibid, Article 398), offence of illegally obtaining of military secret (Ibid, Article 431 (1)), offence of stealing, spying out, purchasing, illegally providing military secret (Ibid, Article 431 (2)), offence of intentionally divulging military secret (Ibid, Article 432), and offence of negligently divulging military secret (Ibid, Article 432).

(2) Information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity, or violates national customs and habits

(c) The act of exploiting the Internet to instigate ethnic hatred, ethnic discrimination, undermine ethnic solidarity (Decision on Maintaining Internet Security, Article 2 (3)), constitutes the offence of instigating ethnic hatred or ethnic discrimination (Penal Law, Article 249).

(d) The acts of exploiting the Internet to organize evil cult organizations, make contact with members of evil cult organizations, undermine the enactment of state law and administrative regulations (Decision on Maintaining Internet Security, Article 2 (4)), constitute the offence of organizing or exploiting superstitious sects and secret societies or evil cult organizations, or exploiting superstitions to undermine the enactment of law (Penal Law, Article 300 (1)), and the offence of organizing or exploiting superstitious sects and secret societies or evil cult organizations, or exploiting superstitions to cause death (Ibid, Article 300 (2)).

(3) Maintaining socialist market economic order and social management order

(e) The acts of exploiting the Internet to marketing false and interior products, or falsely propagate products or services (Decision on Maintaining Internet Security, Article 3 (1)), constitute the offence of producing or marketing false and interior products (Penal Law, Articles 140-150), and offence of false advertising (Ibid, Articles 222 and 231).

(f) The act of exploiting the Internet to damage others' commercial credit or merchandise reputation (Decision on Maintaining Internet Security, Article 3 (2)) constitutes the offence of damaging commercial credit or merchandise reputation (Penal Law, Articles 221 and 231).

(g) The act of exploiting the Internet to infringe others' intellectual property (Decision on Maintaining Internet Security, Article 3 (3)) may be punished according to the offences of infringing trademark right, copyright, patent right or business secret (Penal Law, Articles 213-220).

(h) The act of exploiting the Internet to fabricate and spread false information that influences the transaction of securities or futures, or other information that disorders the financial order (Decision on Maintaining Internet Security, Article 3 (4)), constitutes the offence of manoeuvring transaction price of securities or futures (Penal Law, Article 181).

(i) The act of setup obscene website or webpage, providing link services of obscene website, or spreading obscene books and periodicals, film, phonotape and videotape or pictures (Decision on Maintaining Internet Security, Article 3 (5)), may constitute the offence of creating, duplicating, publishing, selling, or spreading obscene goods to seeking interests (Penal Law, Articles 363 (1) and 366), and the offence of spreading obscene goods (Ibid, Article 364 (1)).

(4) Protecting personal rights, property rights and other legal rights of individuals, corporations and other organizations

(j) Insulting or fabricating facts to libel others with the Internet (Decision on Maintaining Internet Security, Article 4 (1)) constitute offence of insult and libel. Except those gravely endanger the social order and state interests, these offences are disposed only upon charge of the victim (Penal Law, Article 246).

The Temporary Provisions on Internet Publication Management prescribed no Internet publication contents primarily targeting the juveniles may contain contents that induces juveniles to imitate activities breaching social morality or activities of

transgress and crime, as well as the contents of terror, cruelty or other contents that are harmful to juvenile health of body and mind (Temporary Provisions on Internet Publication Management, Article 18). If the Internet publishing institutions publish or transmit these prohibited contents, no criminal liability is prescribed. The illegal income should be confiscated by related authorities. Different sum of fine can also be imposed according to the sum of illegal dealing (Ibid, Article 27).

(iii) Criminalizing the offence of interfering the functioning of computer information systems

Violating the state provision, delete, modify, add, or interfere the functioning of computer information systems, and cause the abnormal functioning of computer information systems, with the grave after-effect, may be punished by imprisonment of less than five years or penal servitude; with specially grave after-effect, may be punished by imprisonment of no less than five years (Penal Law, Article 286 (1)). Decision on Maintaining Internet Security incorporated the act of violating state provisions, interrupt computer networks or communications services without authorization, and cause the computer networks or communications systems unable to function normally (Decision on Maintaining Internet Security, Article 1 (3)).

(iv) Criminalizing offences of destructing data and programs

Violating state provisions, delete, modify or add to the data and applied programs deposited, processed, or transmitted in the computer information systems, with grave after-effect, with the grave after-effect, may be punished by imprisonment of less than five years or penal servitude; with specially grave after-effect, may be punished by imprisonment of no less than five years (Penal Law, Article 286 (2)).

Management Measures of Security Protection of International Networking of Computer Information Networks, and Ordinance on Telecommunications, the above activities are punishable by warning, fine, shut down business no more than six months; grave situation, no more than six months of disconnection and rectification. If necessary, propose the previous institution of issuing the certificate, or examine and approve institution to withdraw the management license or cancel the qualification of networking; if constitutes act violating public security management, punishable according to Ordinance on Public Security Management Sanctions; constitutes crime, held criminally liable according to law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 20).

(v) Criminalizing offence of creating or spreading computer virus

The Management Measures on Computer Virus Prevention (Ministry of Public Security, Management Measures on Computer Virus Prevention, passed on 30 March 2000) prohibit any unit or individual to create (Ibid, Article 5), spread computer virus (Ibid, Article 6), and publish false computer viruses epidemic situation to society (Ibid, Article 7). The activities of spreading computer virus include: intentional input computer virus, threaten the security of computer information systems; provide others with files, software, or media containing computer virus; sell, rent, or present media containing computer virus; other activities of spreading computer virus (Ibid, Article 6). The Management Measures of Security Protection of International Networking of Computer Information Networks prohibit intentional creation or spreading computer virus or other destructive programs (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 6 (4)). Ordinance on Management of Internet Online Services Business Place also prohibits management unit of business place of Internet online services and online consumers to intentionally create or spread computer and other destructive programs, and threaten the security of information networks (Ordinance on Management of Internet Online Services Business Place, Article 15 (1)).

Ordinance on Security Protection of Computer Information System, also prescribed relevant sanction to such activities (Ordinance on Security Protection of Computer Information System, Articles 24 and 20). The Penal Law prescribed that intentional creation or spreading computer virus and other destructive programs, influence the normal functioning of computer system, with grave after-effect, punishable according to the provision on the offence of destructing computer information systems (Penal Law, Article 286 (2)). In Decision on Maintaining Internet Security, the similar provision was restated (Decision on Maintaining Internet Security, Article 1 (2)). Publishing false epidemic situation of computer virus to society, different sums of fine can be imosed to unit and individual (Management Measures on Computer Virus Prevention, Article 17).

(vi) Criminalizing offence committed exploiting computer and the Internet

According to Article 287 of Penal Law, in case where other offences are committed with the factor of computer, the acts should be punished according to the related provisions to deal with. The other articles pf the Penal Law do not contain the contents of “computer”, but they can be committed with the help of a computer. Due

to the validity of the Article 287, such activities have been included into Penal Law.

The Penal Law prescribed that if exploiting computer to commit financial fraud, theft, embezzlement, defalcation, theft of state secret or other offences, punishable according to related provisions of Penal Law (Penal Law, Article 287). Decision on Maintaining Internet Security prohibits theft, fraud, and racketeering exploiting the Internet (Decision on Maintaining Internet Security, Article 4 (3)).

Management Measures of Security Protection of International Networking of Computer Information Networks, the coverage is even broader. No unit and individual may exploit the Internet to threaten state security, divulging state secret, infringe state, social, collective interests and citizens' legal interests or engage in activities of transgress and crime (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 4). The act violating this provision is punishable according to laws and statutes (Ibid, Article 22).

Exploiting the Internet to commit other offences not explicitly listed in Articles1-4 of Decision on Maintaining Internet Security, held criminally liable according to related provisions of Penal Law (Decision on Maintaining Internet Security, Article 5). This article remains the continuation of the spirit of Article 287 of Penal Law, further extending the applying scope to offence committed exploiting the Internet as an instrumentality.

(vii) Criminalizing offence of infringing freedom of communications

The users' freedom and secret of communications are protected by law. No unit or individual may violate the provision of law, exploit the Internet to infringe users' freedom and secret of communications (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 7). The act violating the provisions of law, exploit the Internet to infringe the users' freedom and secret of communications is punishable according to the laws and statutes (Ibid, Article 22).

Decision on Maintaining Internet Security criminalized the act of illegal interception, modification and deletion of others' electronic mail or other data and information, infringing the citizen's freedom and secret of communications (Decision on Maintaining Internet Security, Article 4 (2)).

These situations can apply the related provision in the Penal Law to punish (Penal Law, Article 252). The electronic mail and other data are brought into the field of communications. Internet is only the means of this offence.

(viii) Criminalizing other activities threatening computer information networks

security

Management Measures of Security Protection of International Networking of Computer Information Networks prescribed that violating laws and administrative regulations, any other activities threatening the computer information networks security, should be imposed a warning, fine, or shut down business no more than six months; grave situation, no more than six months of disconnection and rectification. If necessary, propose the previous institution of issuing the certificate, or examine and approve institution to withdraw the management license or cancel the qualification of networking; if constitutes act violating public security management, punishable according to Ordinance on Public Security Management Sanctions; constitutes crime, held criminally liable according to law (Management Measures of Security Protection of International Networking of Computer Information Networks, Article 6 (5) and 20).

Control over the Internet

China has been making efforts to create a giant domestic intranet while barring out the global Internet in order to control the network by central government (Franda 2002, p. 187). The goals of China's operation against online activities are more concentrated on state security than other aspects. The cybersecurity in Chinese context should also be understood as a critical part of state security. The authority tends to view access to information different from the political interests as potential threats to stability and gives no tolerance to it. Thus, free speech bears different meaning from the western notion (Chan 2002). The authorities in China have introduced dozens of laws, rules and regulations normalizing the use of Internet. Traditional agencies have been granted new functions, and new organizations have been established to co-ordinately control the Internet.

In regulating Internet, free speech in the aspect of constitution, and the business information in the aspect of economy cause great anxiety from the enterprises and the human rights organizations.

Direct subject: cyber police

In order to control networks, that is to say, to control users and ISPs, China established cyber police armed with information technology. However, it is necessary

to note that, state security agency is relatively a smaller institution, and is not the only and main organization to control the Internet. The forces of cyber police are surely stronger than the state security agency. Therefore, the actual control over the Internet goes beyond the imagination of the outsiders. Users should always go online with great care for fear that they should be shadowed by the police, listed in the blacklist, and secretly detained and investigated, or publicly arrested. Those who actually violated the laws and regulations might face imprisonment or capital punishment depending on the nature of his guilty.

On the other hand, the actual controllability of the Internet is weak. The early computer networks surveillance in China was hampered by an inefficient computer police force, out-dated computer protection equipment imported in the 1980s and the slow development of computer protection products. Nevertheless, with the growth of the cyber police in number, power, knowledge and technology, experiences, increasing number of websites and messages might be checked and blocked, and increasing number of users might be investigated and arrested.

Major means: blockade of Internet

Once upon a time, Chinese scholars have known blockade as a term in International Law. The term “blockade” of Internet covers a wide scope of meaning, from control over the access to Internet to control over Internet content. Blockade is not only the effect that the illegal contents might be confronted, but also the reason of further legal action when the blockade was breached. Merely breaching the blockade might also incur various levels of punishments. Punishment for unauthorized or inappropriate use of Internet content can take many forms. It may involve lose of permission to use Internet, fines, equipment confiscation and prison terms.

The most efficient way to exercise control over the online activities is through the control over the access to the Internet. As a method of blockade, the shutting down of net cafés is warmly welcomed by the police, who can benefit from it by ways of transferring the computers under their control, or accepting bribes from the owners of the net cafés. Once net cafés were required to provide lists of their customers to the authorities. In addition, thousands of net cafes throughout China have been forced to close in recent years. In other cases, authorities require Internet users to buy personalized identity cards, enabling close monitoring of websites accessed. The users must register personal details such as name, age and address,

which are kept on a central database. The authorities have realised that controlling Internet access effectively is very costly and time consuming but it is still making all attempts to impose regulations.

The government openly attempts to control content. The cyber police are responsible to sniff out and block access to proxy servers located outside China. Chinese government introduced a broad range of new filtering techniques including filtering the keywords. Some online forums and bulletin board system have corresponding self-control mechanism. For example, it is very difficult to publish a message in Qiangguo Forum especially from an abroad computer.

What worries the authorities is that the WWW, email, bulletin board system and instant messages have been used by political dissidents, minority territorial exiles and others to circulate information, and to publicize their cause or to seek supports for online petitions. To deal with all these activities, China is making efforts to cooperate with online giants worldwide to control the flow of information imported to or exported from China over Internet. This kind of cooperation takes place in both routine filtration and case investigation. In order to survive in the specific environment in China, many big online companies adopted strategies in subjection to the official requirements.

Some bulletin board system and forums are strictly limited access within China. In some net cafés, the keepers also screen their machines from browsing foreign websites, including free email service providers in a relatively flexible way. Upon negotiation with the managers, they will authorize the use of the free web-based email systems. Some owners of the net cafés formulate two standards of charge, the lower one for service of limited browsing, and the higher one for service of unlimited browsing, due to the different risks they might face. In China, it is possible to retrieve adult websites, but it is impossible to retrieve political websites with the anti-revolutionary contents. The keepers of the net cafés have also a stake in serving their customers.

Core of the mechanism: joint liability

In the aspect of the system of responsibility of controlling Internet, a system of joint liability has been established, both macroscopically and microscopically, and both in the central and local governments. The responsibility and liability bind all relevant ministries and related basis units. If careless, they can face criminal or

administrative liabilities. These responsibility and liability are regulated in almost all the laws and regulations concerning the control over the networks.

Article 8 of the State Secrets Protection Regulations for Computer Information Systems on Internet stipulates the principle that "responsibility is borne by the person who placed it on Internet." It is the basis for regulating the revelation of state secrets on Internet. However, this does not exempt each ISP's obligation to monitor the Internet. Under Article 10, ISPs, bulletin board system, chat rooms or newsgroup organizers are required to set up their own management mechanisms to assist ensuring that their users transmit no state secret on Internet.

Anyway, this kind of joint liability is nearer to the personal liability in the cases of someone breaching the birth plan. However, if the criminal flees, the liability will be transferred to a certain scapegoat. Chapter IX of Penal Law of China provided the liability for neglecting of duty for government functionaries.

Purpose of regulation: state stability

More people than ever use Internet to express their "anti-revolutionary", "liberalist", and "separatist" tendency, and complaints and discontent. "Chinese people" is not a term that tallies with the Chinese territory. All over the world, there are Chinese who own various national, political and religious views inherited from each historical period. Although the policies of China have taken a big stride toward democracy and freedom within the past 25 years when it carried out reform and openness to the outside world, various views still cannot be in harmony with the official view. In particular, Chinese government has never publicly admitted that it made any of its policy under any outer pressure or in accommodation to the views of any dissident groups.

Free information is not limited to that is useful to commerce and technology. However, in the context of China, regulation of Internet is designed to eliminate harmful information while reserve useful information. Westerners worry that this kind of regulation will have negative influence on the human rights protection and economic development, contrary to the spirit of the Internet.

In fact, besides the action against information breaching the state political interests, China also contributes to maintain the security of information systems. Most of the prosecuted cases have been criminal offences involving embezzlement, fraud, hacking and defacing, and virus spreading.

Negative implications of regulation

People always have scruples when they go online; worrying about that the government prohibits the contents in the web pages retrieved. The laws and the regulations provided only principles on prohibited contents. Users have to judge by themselves whether or not the opened contents are prohibited. For example, if users open an online forum full of messages with various opinions, they must judge at the first sight which category they belong to: separatism, terrorism, dissidents, or national secret. The users can only view all those web pages, then close them with great care, and leave the machine with great panic. This kind of the side psychological effect brought about by the strict regulation frightened many users from goes online.

Critics against the China's substantive law system on cybercrime

The Chinese laws against cybercrime cover a wide range of activities and implement various penalties. However, there are still many loopholes in these previsions. The main problems are: the overlap of the provisions, the missing of the referred regulations and laws, the narrow criminalization, narrow constituents, and laggard penalties. The following present these problems in detail.

The first aspect directs at the overlap of provisions. Article 286 of the Penal Law provides different activities. The first paragraph criminalizes the act of destructing the computer information systems. The second paragraph outlaws the act of destructing system data and applied programs. The third paragraph prohibits the act of intentionally creating and spreading viruses. The former two paragraphs are provided from the aspect of the objects of the act, while the latter one is provided from the aspect of the form of act. By comparing these three paragraphs, we can find that they are intercrossed. Generally, creating and spreading computer viruses could result in the abnormal operation of the systems, and could also destruct data and applied programs in the systems. At present, most of the abnormal operation of the computer systems and the destruction of data and applied programs are committed by computer viruses. This results in the simultaneous application of the two paragraphs. Scholars proposed the solution to this problem by disseminating this Article into two different offences, one is direct destruction of computer systems, and the other is destruction with the computer viruses.

The second aspect mentions the legal gaps formed in referring to other laws and regulations. Compared with Convention on Cybercrime, the laws and regulations on cybercrime in fact fully criminalize the activities covered by the Convention. These laws and regulations outlaw various cybercrime and give appropriate punishments, including public security management punishments, administrative punishment, penalty and measures limiting the qualification of holding a post. The problems are that when the nature and situation of these criminalized activities are grave, they should be punished by penal law. When the penal law is not complete, the provision "holding criminally liable according to law" becomes invalid. The possible problem is that the lighter cybercrime (transgress) will be imposed public security management punishment or administrative punishment, while some of the graver cybercrime (crime) cannot be held "criminally liable" "according to law."

The third aspect is concerning the narrow scope of criminalization. Huang and Chen (2005) pointed out that Article 285 of the Penal Law limits the objects of the offence to the computer information systems of national affairs, construction of national defence, and the field of top science and technology. With the development of the Internet, the security of other computer information systems is also necessary to protect. Therefore, the protection scope should be extended (Huang and Chen 2005).

The fourth aspect critisizes the narrow legal constituents. According to Penal Law, the subject of computer crime is limited to natural person. The corporate liability should be added (Huang and Chen 2005). According to Article 17 (2), a person who is older than 14 years old but younger than 16 years old, is only criminally liable for eight kinds of severe offences: intentional homicide, intentional injury resulting in grave bodily harm and death, forcible rape, robbery, sales of drug, arson, explosion, and spread poison. Many of the perpetrators of cybercrime are younger than 16 years old. Some scholars proposed that the subject scope of the cybercrime should be extended, that is to say, applying a lower liable age. Nevertheless, other worry that this does not coincides with the trend of humanism of penal law.

Finally, the laggard penalty provision is also a focus of criticism. Huang and Chen (2005) also pointed out that the Articles 285 and 286 of Penal Law provide the imprisonment as the only punishment for offence against information systems, absent of fine and disqualification. In many other countries, the penalty may include all of

the three kinds. From the deterrent effect, the Chinese law should be amended to add punishments other than imprisonment (Huang and Chen 2005).

International criminal justice assistance

In the aspect of international coordination and assistance, China's step is limited. China did not sign the Convention on Cybercrime. In other international cooperative actions, China played not so much a role. China concluded criminal justice assistance agreements with Egypt, United Arab Emirates, Pakistan, Belarus, Bulgaria, Poland, Korea, Russia, the Philippines, Columbia, Cuba, Kazakhstan, Kyrgyz, Canada, Cambodia, Latvia, Lesotho, Laos, Lithuania, Romania, Mongolia, Peru, South Africa, Tajikistan, Thailand, Tunisia, Ukraine, Uzbekistan, Vietnam, and the United States (Summarized according to the bilateral agreements collected on non-official Law Library website, http://www.law-lib.com). However, as many other traditional international agreements, it is not so clear concerning whether these agreements can work in prosecuting trans-national cybercrime.

Conclusion

In the control over the Internet, China took a series of actions characterized by content filtering and activity monitoring, in order to maintain the state stability, as well as cyber security. The recruitment of cyber police, the investment on security technology, the requirements on the Internet enterprises, and the surveillance on the users, form a close net to prevent cybercrime from happening.

The countermeasures that China took to fight against cybercrime have commonness with other countries. First, criminalisation has been a significant way to incorporate the actions into the legal framework. Notwithstanding the difference with regard to the social system, the legal framework in China is developing with a modernized manner. The penal law is nothing exceptional. The 1997 amendment of penal law and a series of regulations formed the systematic legal system against cybercrime. Second, the Chinese law covers most of the cybercrime offences that have been criminalized in industrialised countries and imposes certain punishment. Therefore, if there is the necessity of international coordination between China and other countries, the substantive law basis is somewhat ready. Furthermore, the

Chinese control over the Internet is not without precedents. In practice, many control measures adopted in China are similar to those in the United States and European countries.

Certainly, the control mode in China has its speciality. First, the focuses of the actions in China are characterised by maintaining state stability and social order. The focus of all focuses is on the online speech that breaches the state regulation. The anxiety of the authorities is that the absolute free speech would erode the foundation of state politics. The criminalisation of content-related offences has the unparalleled coverage than other countries. Second, the Chinese legal system is more flexible than many other countries. The forms (or "sources" in jurisprudence) of laws are diversiform, including penal code, special statutes, legislative and judicial interpretations, and administrative regulations, all being integrative parts of the criminalization. Third, combat and prevention are designed to combine with each other. The preventive system does not prevent from potential cybercrime but also detect the occurrence of offence. Fourth, strike-hard strategy is used on occasion. The strike-hard strategy has been used in China since early 1980s to clamp down the rising waves of crime. At present, this strategy is also used in fighting against various specific crimes, including offences endangering public order, offences of illegal publications, offences related to pornographic materials, etc. Generally, various computer and Internet-related offences are fought together with the content-related offences in strike-hard actions.

References

Chan, J. M. 2002. Media, Democracy and Globalization: A Comparative Perspective, January. Retrieved 14 January 2009, from http://www.wacc.org.uk/wacc/content/pdf/680

China Internet Network Information Center. 2006.*17th Statistical Survey Report on the Internet Development in China*, January.

Clarke, D. 1999. Private Enforcement of Intellectual Property Rights in China, in *Intellectual Property Rights in China: Evolving Business and Legal Frameworks*, Volume 10, Number 2, National Bureau of Research Analysis.

Dai, Xiudian. 2003. ICTs in China's Development Strategy, in Hughs, Christopher R.and Wacker, Gudrun, eds. *China and the Internet: Politics of the*

Digital Leap Forward, New York, New York: RoutledgeCurzon, pp. 8-29.

Franda, Marcus. 2002. *Launching Into Cyberspace: Internet Development and Politics in Five World Regions*, London: Lynne Rienner Publishers.

Han, Qiao and Meng, Na. 2004. Penal Law Experts: China Has Insufficient Legal Basis in Combating Cybercrime, 20 September, *Great Wall Online*. Retrieved 14 January 2009, from http://www.hebei.com.cn/node2/node1302/daji/gdpl/userobject1ai260765.html

Huang, Zelin and Chen, Xiaobiao. 2005. The Defects of Criminal Law Regulation and Theoretical Reaction to Computer Crime, *Jianghai Xuekan*, Issue 3, pp. 112-118.

Huasheng Newspaper. 1999. Computer Crime in China Increased 7-Fold in One Year, 30 July.

Kim, M. W. 1997. How Countries Handle Computer Crime, *Ethics and Law on the Electronic Frontier*.

Li, Xingan. 1992. A Study on the Application of Criminal Law to Computer Crime, China University of Political Science and Law Graduate Law Review.

Ministry of Public Security. 2005. China Ministry of Public Security Enacted "Provisions on Technical Measures of Internet Security Protection," 30 December.

Sunergy Beijing. 1997. The Internet in China: A Modern Tool in an Ancient Land, 19 November. Retrieved 14 January 2009, from http://www.sun.com/sunergy/archives/beijingtrans.html

Chapter VIII International Platform for Tackling Cybercrime

Abstract

This article reviews the international impetus of criminal law reform in combating cybercrime. This article classifies actions of international harmonization into professional, regional, multinational and global actions, summarizes the major concerns of these actions, and concludes the influence of the Convention on Cybercrime on state and international levels of legal countermeasure. The article also points out the limitations of the previous actions and anticipates the United Nations to play a more important role.

Keywords: International harmonization, Cybercrime, Legal system

Introduction

Traditionally, crime and punishment are largely local, regional, or national. Today, many differences confronting us are associated with the transnational character of cybercrimes. It is therefore important to have international legal instruments ready to serve anti-crime efforts.

This article inspects international harmonising efforts to accommodate legal fight against cybercrime, categorising the actions into four aspects: professional law enforcement efforts, regional efforts, multi-national efforts, and global international efforts. Subsequently, the article also categorizes the international actions according to the subject matters into additional aspects, including promotion of security awareness at both international and national levels, harmonization of legislations, coordination and cooperation between law enforcement agencies, and direct anti-cybercrime actions. The article will also examine the nations' attitudes toward the Convention on Cybercrime. Based on the analysis, the article will briefly evaluate the effectiveness of previous international harmonization.

From domestic legislation to international harmonization

People usually are impressed by the illusory overlap between the Internet space and international space. Notwithstanding information systems are linking continents, islands, residents and communities into a giant virtual network, states and areas reserve their traditional sovereignty. McConnell International's metaphor (McConnell International 2000, p. 8) said that: "In the networked world, no island is an island." At this turning point, the globally connected Internet has made cybercrime a trans-border problem. The "international dimension" (Wasik 1991, pp. 187-201), "trans-national dimension" (Sofaer and Goodman 2005) or "global dimension"(Grabosky 2004, pp. 146-157) of cybercrime is universally perceived. While law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures merely will be critical but not perfect for meeting this worldwide challenge. International coordination and cooperation are necessary in fighting against offences commonly prohibited by every country.

Many international organizations have been making efforts to harmonize actions within their forums. Many authors have also been pursuing research on the international harmonization from different standpoints and for different goals, for example, Sieber (1996; 1998), United Nations Crime and Justice Information Network (UNCJIN) (1999), Police Commissioners' Conference Electronic Crime Working Party (2000), Sofaer and co-workers (2000), Putman and Elliott (2001, pp. 35-68), Schjoberg (2005), and so on. Although information about the basic facts of international harmonization that these researches deal with is the same, different knowledge can be drawn with different thinking. For the purpose of convenient summarization within this article, I categorize the international harmonization actions into the following groups: professional organization, regional organizations, multi-national organizations, and global organizations. Many other valuable international actions have not been considered merely due to the limit of this study (possibly any studies on cybercrime cannot cover all useful international actions of international organizations on all scales).

Professional efforts of International Criminal Police Organization (Interpol)

Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues, such as Interpol,

International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cybersecurity protection and cybercrime prevention. Although some other organizations also greatly contribute to coordinating cybersecurity protection, their emphasis is not necessarily on law. By this standard, this section only analyzes the actions of International Criminal Police Organization (Interpol) (For a general analysis of Interpol as "a world crime-fighting organization that has puzzled three generations of scholars, law-enforcement officers, and legislations," see Fooner 1989).

As an international law enforcement organization with 184 members, Interpol started to tackle computer crime very early, coordinating law enforcement agencies and legislations, in the respects of which Interpol made efforts to improve counter-cybercrime capacity on international level. A 1981 survey of members on cybercriminal law recognized dilemmas in application of existing legislation (Schjoberg and Tingrett 2004). Based on the recognition of the legal gaps between countries, and gaps between legal framework and criminal phenomenon, Interpol expanded its task to both law enforcement and legal harmonization.

Currently, there are four working parties within the framework of Interpol, including African, American, Asia-South Pacific and European Working Parties on Information Technology Crime. Besides these groups, Steering Committee for Information Technology Crime was established in order to harmonize the different regional working party initiatives (See Interpol web site for detailed introduction to the functions and activities of these working parties and the steering committee, at http://www.interpol.net/Public/TechnologyCrime/WorkingParties/Default.asp). Considering the ready harmonized legislation as the prerequisite for the coordinated law enforcement, the African Working Party agreed upon "the project on legislation and comparative law existing in the African with a view to have more African states co-signing and/or ratifying the Council of Europe Cybercrime Convention."(Ibid.) Apparently, legal harmonization is one of Interpol's important tasks in working towards an effective law enforcement environment.

In the aspect of law enforcement, Interpol provided a technical guidance in cybercrime detection, investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European Working Party on Information Technology Crime (Ibid.). Compared with the substantive and procedural law harmonization of today's Convention on Cybercrime, the Manual

developed a technological law enforcement model in improving efficiency of combating cybercrime.

Along with the efforts in law enforcement on cybercrime, Interpol also takes actions to directly prevent cybercrime, cooperating with credit card companies to combat payment fraud, building a database on Interpol's web site (Police Commissioners' Conference Electronic Crime Working Party2004). As one of the necessary cooperation projects at international level of law enforcement, cybercrime and other trans-border crimes are specially dealt with by Interpol in gathering and sharing information. In addition, Interpol is making efforts to establish the network to harvest information relating to activities on the Internet (Interpol, Interpol press release, CPN02/00/COMandPR, 5 February 2001).

Regional efforts

There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cybersecurity and harmonize international measures to combat cybercrime. This section will only introduce four of these organizations, which have taken typical actions in combating cybercrime.

(i) The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime (APEC, *Conference Report: Cybercrime Legislation and Enforcement Capacity Building Project*, (Bangkok, Thailand, 21-25 July 2003)). The APEC conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where advanced the APEC economies support other member economies in training legislative and investigative personnel (Cybercrime Expert Group, Proposal, Doc no: telwg29/ESTC/12, APEC Telecommunications and Information Working Group 29th Meeting (Hong Kong, China, 21-26 March 2004).

After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure (APEC Leaders

Statement on Counter-terrorism, APEC Economic Leaders' Meeting (Shanghai, 21 October 2001)).

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002 (APEC, Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy, 2002/CSOM/052, Concluding Senior Officials Meeting (Los Cabos, B.C.S., Mexico, 21-22 October, 2002)), supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting made a recommendation concluded six areas that can serve as the foundation for the APEC's endeavour for cybercrime prevention, including legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security (Ibid.). The Ministers and Leaders of the APEC have made a commitment to "endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003." (Cybercrime Expert Group, Proposal, Doc no: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting (Hong Kong, China, 21-26 March 2004))

In response to this call from leaders, a survey of laws was carried out and a summary was made to conclude the responses from member economies received in 2003 (E-Security Task Group, Cybercrime Legislation and Enforcement Capacity Building Project (Bangkok Thailand, 21-25 July 2003)). Economies proposed corresponding projects in information security task groups. For example, the U. S. proposed a project in the e-Security Task Group of the Telecommunications and Information Working Group. The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was held from 21-25 July in Bangkok, Thailand, attended by over 120 delegates from 17 economies. The objectives of the meeting are to assist economies to develop necessary legal frameworks; to promote the development of law enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime (See APEC, Cyber Security Workshop Summary, 2003/SOMIII/ECSG/021, Electronic Commerce Steering Group Meeting (Phuket, Thailand 15-16 August 2003)). On the conference, experts

agreed that every economy need a legal framework including substantive and procedural law, and law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional cooperation, law enforcement construction, and capacity building of investigators (APEC, Conference on the Strengthening International Law Enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors, Media Release (Bangkok, 25 July 2003)).

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed Lima Declaration, "encouraging all economies to study the Convention on Cybercrime (2001) and endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)." (Article 26 of Lima declaration, The 6th APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMING, 1-3 June, 2005, Lima, Peru)). However, due to great difference between member economies within the APEC, the development toward unified legal instruments is not so satisfactory. Although some economies claimed that their laws had been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalising cybercrime.

The efforts are still to be made in the forum of the APEC to address cybercrime. The U. S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop the curriculum by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors) (APEC, 2006 Budget – Operational Account Project: TEL 04/2006 – Judge and Prosecutor Cybercrime Capacity Building Project, 2006/BMC1/012-6, Budget and Management Committee Meeting I, APEC Secretariat (Singapore, 29-30 March 2006)).

Recognizing that the use of information and communications networks and services exposes all of us to a broad range of risks, which affects the integrity of our information systems and our safety and security as well as our confidence in their use, and noting that a trusted and secure on-line environment is fundamental to facilitate electronic transactions, 2008 APEC Telecommunications and Information Ministerial Meeting (The Seventh APEC Ministerial Meeting on The telecommunications and information industry (TELMIN7), 23-25 April 2008,

Bangkok, Thailand) published “Bangkok Declaration: Digital Prosperity: Turning Challenges into Achievement,” advocating to for promoting a safe and trusted ICT environment for digital prosperity, in which a key priority would be the development of effective responses to ensure security against cyber threats, malicious attacks and spam. The declaration called for ongoing efforts to provide users including SMEs within APEC economies with the knowledge and skills they need to deal effectively with these threats and to cultivate a culture of security. The Declaration also encouraged continued sharing of information, experiences and practices on the protection of electronic information systems of essential infrastructure and services (Paragraph 16). The Declaration emphasized enhancing outreach activities on cybersecurity, which is regarded as a global and cross-jurisdictional problem which requires governments, law enforcement agencies, industries, business and consumers to work together across borders to develop multilateral approaches. Therefore, the meeting recognized the need not only to develop and implement domestic cyber security strategies but also to build cross-border collaboration between economies and cooperative work between APEC and other organizations on security initiatives (Paragraph 17). The Meeting commended economies to facilitate the work of key stakeholders including Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), law enforcement officials, legislators and others to combat malicious attacks and enhance cyber security (Paragraph 18). The Meeting also commended the collaboration with other international organizations to share experiences and develop best practice approaches to cyber security and to enhance collective security (Paragraph 19). The Meeting stressed the need for ongoing efforts that will assist governments and the private sector to work together to combine innovation with security, and to protect electronic information systems of essential infrastructure and services. In particular, the Meeting encouraged economies to undertake training and exercises designed to enhance response capabilities and to test continuity and contingency plans in the event of a cyber attack (Paragraph 20).

In December 2008, APEC Telecommunications and Information Working Group published “Guide on Policy and Technical Approaches against Botnet,” the main object is to raise the APEC economies’ awareness on Botnets, improve capabilities of each APEC members for Botnet attribution and response, and to promote local, regional and international collaboration. The report defined Botnet as

created by the attacker (Botmaster) for a specific purpose, through various ways to infect vulnerable hosts as many as possible, and using command and control mechanism to control the large number of hosts (Bot) on the Internet (National Computer Emergency Response technical Team/Coordination Centre of China (CNCERT/CC) 2008, p. 8). The report reviewed the evolution of Botnet and described the Botnet structure, and presented four types of Botnet classified by different command and control mechanism, including Botnet based on IRC, HTTP and P2P. The report introduced the current status of Botnets in the world as well as the main difficulties of combating Botnets. The report developed a suit of guidelines against Botnets from the perspective of government, industry, and individual users respectively: For government, the recommendations consist of governmental staff training, policies making, information sharing, public education, and global cooperation promotion; for industry, we provided some guidelines for ISPs (Internet Service Providers), network security vendors, and common enterprises; and for individual users, the report suggested some self-prevention and detection methods and listed a few existing Anti-Botnet products. The report presented five best practices related to combating Botnet. The first two, fighting for DDoS attack to Feixing website and eliminating MocBot Botnet, are the real countermeasures against Botnet taken by CNCERT/CC. The third practice, Cyber Clean Centre is an organization in Japan, which is active in analyzing characteristics of Bots and providing information on disinfestations of Bots from users' computers. The last two are specific practices of tracking Botnet based on two different technologies: Honeynet and Mwcollect (National Computer Emergency Response technical Team/Coordination Centre of China (CNCERT/CC) 2008, pp. 1-2).

(ii) The Council of Europe (COE)

The Council of Europe has been working to tackle the rising international anxiety over the risks brought about by automatic processing of personal data since early 1980s (For example, the Committee of Ministers of the Council of Europe adopted Recommendation R (89) 9 of the Council of Europe on computer-related crime, which contained guidelines for national legislatures, on 13 September, 1989). In 1981, Council of Europe implemented Convention for the Protection of Individuals with Regard to Automatic Processing of personal data (ETS No. 108, 26 January 1981), which was revised according to Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and Additional Protocol to Convention ETS

No. 108 on Supervisory Authorities and Trans-border data Flows, 8 June 2000. The Convention recognizes the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing," and the necessity "to reconcile the fundamental values of the respect to privacy and the free flow of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

Chapter II of the Convention established basic principles for data protection, one of which is data security (Article 7):

"Appropriate security measures shall be taken to for the protection of personal data stored in automated data files against accidental or unauthorized access, alteration or dissemination."

The expert committee appointed in 1985 published Recommendations of 1989 and 1995, addressing the issues of substantive laws and procedural law in this area respectively (See Recommendation No. R. (95) 13).

Recommendation R. No. (89) 9 recognized the importance of an adequate and quick response to the new challenge of computer-related crime, which often has a trans-border character, and recommended the governments to consider the report on computer-related crime by the European committee on Crime problems.

Recommendation No. (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. The Recommendation recognized that information systems may also be used for committing criminal offences, evidence of criminal offences may be stored and transferred by these systems, and criminal procedure law of member states often do not provide for appropriate powers to search and collect evidence in these systems during the criminal investigation. Appendix to the recommendation provides principles for criminal procedure laws on search and seize, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption in research, statistics and training, and international cooperation.

In 1997, the Council of Europe began drafting the Convention on Cybercrime, which was open for signature in 2001 and took effect in 2004 (See Council of Europe, Convention on Cybercrime, CETS No.185, status as of 18 August 2007). In 2003, Additional Protocol to the Convention on Cybercrime Concerning the

Criminalization of Acts of a Racist and Xenophobia Nature Committed Through Computer System (ETS NO. 189) was implemented. The Convention addresses substantive law, procedural law, jurisdiction, and international law in the field of cybercrime. The Convention is a historic landmark in the combat against cybercrime. It is expected that the Convention will firstly have deep impact on the legal reform relating to cybercrime on its 46 member states and one candidate state.

On the 2004 Conference on Cybercrime, the Council of Europe called for “wide and rapid” access to and “effective implementation” of the Convention on Cybercrime, raising awareness on the highest political level, and encouraging cooperation between public and private sectors (Council of Europe, Conference on The Challenge of Cybercrime (Palais de l'Europe, Strasbourg, France, 15-17 September 2004)).

On the 2005 Conference on Cybercrime, the Council of Europe expressed concern about the fast increasing threats and serious social and economic results of cybercrime including terrorist activity on the Internet, noted that most cybercrime is international cybercrime, recognized the need for effective and compatible laws and tools to enable efficient cooperation to combat cybercrime, called upon public and private cooperation, and encouraged access to the Convention on Cybercrime (Council of Europe, Cybercrime: A Global Challenge, A Global Response (Casa de America, Madrid, Spain, 12-13 December 2005)).

In 2006, the Council of Europe launched a Project against Cybercrime, intended to:

“Assistance to the development of national legislation in line with the provision of the Convention; training of judges, prosecutors and law enforcement officers in the investigation, prosecution and adjudication of cybercrime; training of criminal justice officials and 24/5 contact points in international cooperation on cybercrime.”

(iii) The European Union

The EU took a series of actions to tackle cybercrime through impelling the coordinated law enforcement and legal harmonization. The civil liberty has also been a focus in the anti-cybercrime field.

In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural person (Article 2(a)). The scope of the

Directive is limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive requires that appropriate technical and organizational measures must be implemented

"To protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." (Article 17-1)

The Directive requires the Member States provide administrative and judicial remedies for the victim (Article 22), and compensation liability of (Article 23) and the sanctions on (Article 24) the breacher.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. The Directive furthers the protection implemented in the Directive 95/46/EC, and is aimed at providing for the harmonization of the Member States' provision to attain an equivalent level of protection (Article 1-1). The Directive extends the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive is limited to the processing of personal data relating to the provision of publicly available telecommunications services in public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing system, the Directive 97/66/EC emphasize the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not Member States) "to take appropriate technical and organizational measures to safeguard security of its services" (Article 4-1). The Directive requires the Member States to implement regulations to ensure the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails.

On 27 November 2001, a plenary session took place in Brussels of the EU Forum on Cybercrime, organized by the EC (European Commission, EU Forum on Cybercrime, Plenary session (Brussels, November 27, 2001)), primarily discussed about

retention of traffic data (EU Forum on Cybercrime 2001).

In April 2002, the Commission of the European Communities presented a Proposal for a Council Framework Decision on Attacks against Information Systems, which formed the Decision on 24 February 2005 (Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 069, 16/03/2005 P. 0067 – 0071). The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting and attempt of these offences (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against "information systems with specific protection measures in place and must be for economic gain." (Article 2)

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against Information Systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." (Ibid.) Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interruption" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempt of these offences, but require member states take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the penalties for illegal system interference and illegal data interference as punishable by criminal penalties of a maximum of at least between one and three years of imprisonment (Article 6.2). As for the "aggravating circumstances", the criminal carries a maximum of at least between two and five years imprisonment (Article 7.1). These aggravating circumstances include the organized attack, and the attack that "caused serious damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more

persons, acting in concerted manner with a view of committing offences." (Article 1, Joint Action 98/733/JHA of 21 December, 1998 adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Official Journal L 351 (29 December, 1998))

It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime (HE 153/2006, Detailed Justifications, 2. Framework Decision and Valid Legislation). After revision of the legislation required by the Convention, national law (of Finland) will also meet the demand of the Framework Decision (Ibid.). Today, comprised of 27 member states and three candidate countries, the EU remains active in addressing cybercrime.

(iv) The Organization of American States (OAS)

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cybercrime. Through its forum for the Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA), OAS has long recognized the central role that a sound legal framework plays in combating cybercrime and protecting the Internet. Such recognition prompted the REMJA to recommend the creation of the Group of Governmental Experts on Cybercrime (The Group of Experts) in March 1999 (Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II), Chapter V). The Group of Experts has been devoted to analyze cybercrimes, to inspect the domestic cybercrime law, and to find cooperation ways in the Inter-American system to combat cybercrime. The Group of Experts has held four meetings (The First Meeting and Second Meeting were held in May and October 1999, separately, the Third Meeting in June 2003, the Fourth meeting in February 2006, all in Washington D. C. U. S. See OAS web site, at http://www.oas.org/juridico/english/cyber_experts.htm).

The Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA III) (Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA III), Chapter IV) urged member states to take steps to endorse cybercrime law; harmonize cybercrime laws to make international cooperation possible. The Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA V) (Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA V), Appendix I) recommends that Member States evaluate the advisability of implementing the principles of the Convention on Cybercrime, and consider the possibility of acceding to that

convention.

In 2004, the Fourth Plenary Session of the Organization of American States General Assembly passed the resolution on "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, " proposing that "An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry." (AG/RES. 2040 (XXXIV-O/04), Adopted at the fourth plenary session of the Organization of American States General Assembly held on 8 June 2004 in Quito, Ecuador).

IV Meeting of the Group of Governmental Experts on Cyber-Crime was held in Washington DC, 27-28 February, 2006. The Meeting recommended taking steps as soon as possible to implement the recommendations in this area adopted by this Group at its third meeting and by REMJA-V; prior to REMJA-VI, providing the OAS General Secretariat with information identifying the authorities that are to serve as points of contact for international cooperation in the area of cyber-crime; the OAS General Secretariat consolidate a single directory of these points of contact; continuing to make progress with adopting laws, adapting existing legislation, or taking other steps necessary to effectively fight against cyber-crime, taking into consideration the contributions of those workshops; developing a training program to facilitate their link-up with the "24 hour/7 day emergency network" set up by the G-8; examining mechanisms to facilitate broad and effective mutual cooperation in combating cyber-crime and study, where possible, the development of technical and legal capacity to become part of the 24/7 network set up by the G-8 to help conduct cyber-crime investigations; strengthening an inter-American cooperation portal on the subject be further pursued, with one part for the public and another part with restricted access for government officials working in this field; continuing to compile in a systematized fashion the cyber-crime laws of the OAS member states, including their substantive and procedural aspects as well as the area of mutual legal assistance, and making this information available to the OAS member states on the Internet webpage, so that that information may be used, among other purposes, for training in the area; drawing up an inventory of the most common forms and means of cyber-crime in the member states, disseminate it through the private "Internet" page, and present it to the group of experts at its next meeting for consideration; considering to

applying the principles of the Council of Europe's Convention on Cyber-crime and to adhering thereto, and to adopting the legal and other measures required for its implementation. Similarly, the continued strengthening of mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cyber-crime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the OECD, the G-8, the Commonwealth, and INTERPOL, in order for the OAS member states to take advantage of progress in those forums; further developing the partnership between the private sector and the officials responsible for investigating and prosecuting such crimes; supplying training in the area of cyber-crime and management of electronic evidence to OAS states; encouraging the use of E-learning programs that allow for the ongoing training of governmental experts in the forensic handling of electronic evidence (Recommendations, pp. 1-2).

V Meeting of the Group of Government Experts on Cyber-Crime was held in Washington, DC, 19-20 November 2007. The Meeting recommended establishing specific units or bodies charged with the direction and development of the investigation and prosecution of cyber-crime, and that they be assigned the necessary human, financial and technical resources in order to carry out their functions in an efficient, effective and expeditious manner; providing the OAS General Secretariat with information identifying the prosecutorial and police authorities that serve as points of contact for international cooperation for cyber-crime and electronic evidence matter; examining their legal systems and adopt the specific legislation and procedural measures necessary to criminalize the different modalities of cyber-crimes, ensure the efficient, effective and timely investigation and persecution of those crimes, and enables states to cooperate with each other in the investigation and prosecution of cyber-crimes; adopting legislation and procedural measures necessary to ensure the collection and safe custody of all forms of electronic evidence, enable to assist each other in matters involving electronic evidence and their admissibility in criminal proceedings and trials, including the development of provisions for service providers which guarantee the preservation and recovery of information that is stored or in transit; taking the measures necessary to join the G-8 "24 hours/7days Emergency Network of Contacts for High Tech Crime" (Recommendations, pp. 1-2).

Multi-national efforts

Unlike professional organizations that are limited to a more specific field of concern, and unlike regional organizations that are limited to a more specific location of states, the multi-national international organizations care affairs in a broader range and take actions in a broader territorial scope. This section presents the efforts of three of the multi-national organizations.

(i) The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in harmonizing laws of the member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" (Richard Bourne, 2002 Commonwealth Law Ministers' Meeting: Policy Brief (Lodon: Commonwealth Policy Studies Unit, 2002) 17). Within the Commonwealth's 53 member countries, the "Model Law" has wide influence on the domestic legislation. Through this model law, the Convention on Cybercrime has become one of the legislative choices in the aspect of substantive criminal law, covering the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and child pornography.

Compared with the Convention on Cybercrime, the Model Law expanded criminal liability for the offences of interfering with data, interfering with computer systems, and illegal devices to include reckless liability. The Model Law also considered the problem of dual criminality with the wording of that the act applies to an act done or an omission made by a national of a state outside its territory, if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This may lead to prosecution or extradition based on dual criminality, but not extradition as it is provided in Convention on Cybercrime (Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean, Kingston, Jamaica, 3-7 November, 2003, published in January, 2004).

Some of the Member countries of the Commonwealth have made efforts to draft domestic law according to the model law, such as Bahamas and St. Lucia (Ibid.). In Barbados, Belize, and Guyana, the Model Law would be considered as a guide to the enactment of similar legislation (Ibid.). However, in many other countries, there is still no legislation specialized on cybercrime (Ibid.).

Besides impelling legislation within the forum, another focus of the

Commonwealth is on mutual assistance in law enforcement between Commonwealth member states and between Commonwealth member states and non-Commonwealth states. In 2005 Meeting of Commonwealth Law Ministers and Senior Officials, the Expert Working Group proposed 10 recommendations for member states to adopt suitable measures in improving domestic law enforcement and trans-national assistance, and encouraged member states to sign, ratify, accede to and implement the Convention on Cybercrime as a basis for mutual legal assistance between Commonwealth member states and non-Commonwealth states (Commonwealth Secretariat, The Harare Scheme on Mutual Assistance in Criminal Matters: Possible Amendments to the Scheme and Discussion of Interception of Communications and Related Matters, Meeting of Commonwealth Law Ministers and Senior Officials, Annex 1: Summary of recommendations of the Expert Working Group, R4 (Accra, Ghana, 17-20 October 2005.): 5).

(ii) The Group of Eight (G8)

Since mid-1990s, the Group of Eight (G8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the Halifax Summit 1995, the Group of Seven recognized "that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime." (G7, Chairman's Statement, 17 June 1995, Halifax Summit (15-17 June 1995)). The group released a 40 point "recommendations to combat Trans-national Organized Crime efficiently" at the G7/P8 Lyon Summit, urged the states to increase criminalization, prosecution, investigation, and international cooperation, while completely consider the human rights protection (P8 Senior Experts Group, 40 recommendations to Combat Trans-national Organized Crime, Paris, 12 April 1996, Reference: 1996CIIa5).

At the Denver Summit 1997, the Group of Eight proposed to strengthen efforts to realize the Lyon recommendations, concentrating on punishing high-tech criminals, and promoting the governments' technical and legal abilities to react to trans-territorial computer crimes (G8, Communiqué, Denver, 22 June 1997, Denver Summit of the Eight (20-22 June 1997)). The Group of Eight Meeting of Justice and Interior Ministers of December 1997 responded to increased international movement and use of ICT by criminals, organized crime, and terrorists (December 1997, the G8 Meeting of Justice and Interior Ministers). Ministers noted, in a Statement of Principles

concerning electronic crime, that, while criminal legislation is national responsibility, the character of the information networks obstructs the countries from operating traditional power over this problem. Domestic legislations must be complemented by international cooperation to criminalize abuse of the networks and harmonize the investigation action (Ibid.).

At the subsequent summits in the following years, the Group of Eight repeatedly expressed their concern about cybercriminality. At the Okinawa Summit, the Okinawa Charter on Global Information Society consented international collaboration and harmonization about cybercrime. "In order to maximize the social and economic benefits of the information society", the Group of Eight agreed on the principles and approaches of the concern of privacy protection, free flow of information, and security of transactions (G8, Okinawa Charter on Global Information Society, (Okinawa, 22 July 2000)).

The charter recognized that security of the information society necessitates coordinated action and effective policy responses (Ibid.).

(iii) The Organization for Economic Cooperation and Development (OECD)

With its 30 member countries, the OECD addresses computer security for several decades. In 1983, an expert committee was appointed by OECD to discuss computer crime phenomenon and criminal law reform (S. Schjoberg and A. M. Hubbard, Harmonizing National Legal Approaches in Cybercrime, International Telecommunication Union, WSIS Thematis Meeting on Cybersecurity (Geneva, 28 June-1 July 2005)). The offences against confidentiality, integrity or availability listed in the 1985 OECD document include unauthorized access, damage to computer data or computer programs, computer sabotage, unauthorized interception, and computer espionage (Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986. Cited in UN, Crimes related to Computer Networks: background Paper for the Workshop on Crimes Related to the Computer network, Tenth UN Congress on the Prevention of crime and the treatment of Offenders (Vienna, 10-17 April 2000)). In December 1999, the OECD officially approved the Guidelines for Consumer Protection in the Context of Electronic Commerce (U. S. Department of Justice, *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet*-- *A Report of the President's Working Group on Unlawful Conduct on the Internet (2000):* 27), representing member states' consensus in the area of consumer protection for e-commerce: consumers should be protected in e-commerce not less than that within traditional commerce (Ibid.). OECD

adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to “establish a heightened priority for security planning and management”, and to “promote a culture of security among all participants as a means of protecting information systems and networks.” (Organization for Economic Cooperation and Development, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Part I (2000)).

The Guidelines are designed to:

“Promote a culture of security among all participants as a means of protecting information systems and networks.

Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the requirement for their adoption and implementation.

Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.

Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.

Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.

Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.” (Ibid, Part II).

The Guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (OECD 2002a, Part III). Because of the nature of the guidelines and the distance from the legal actions, the practical endeavours are left to the member countries to make.

Global international efforts by the United Nations (UN)

In certain sense, there are numerous global organizations. Nevertheless, the UN

is capable of being identified as the only global organization that forms a forum of its 191 member states with fuller functions. Compared with professional organizations, the UN does not limit its activities to certain domains. Compared with regional organizations, the UN does not limit its activities to certain states (in the field of cybersecurity protection and cybercrime prevention). The actions of the UN have unique advantages in coordinating international positions.

In 1985, General Assembly Resolution 40/71 of 11 December called upon Governments and international organizations to take action in conformity with the recommendation of the commission on the legal value of computer records of 1985, in order to ensure legal security in the background of the broadest possible use of information processing in international transaction (See UN General Assembly Resolution A/RES/51/162 (30 January 1997)).

In 1990, the General Assembly of the UN adopted the Guidelines Concerning Computerized Personal Data Files. It proposed that:

"Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses."

The Guidelines extended the protection of governmental international organizations (Part B).

"The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime" called for further international work and presented a proper statement of the problem. It stated that at the international level, further activities can be undertaken, including harmonising substantive law, and establishing a jurisdictional base (United Nations Crime and Justice Information Network (1999), Paragraph 295).

The background paper for the workshop on crimes relating to the computer network at the Tenth UN Congress on Prevention of Crime and Treatment of Offenders proposed two levels of definition of cybercrime: In the narrow sense, that is, the strict computer crime, refers to "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them." In the broad sense, that is, computer-related crime denotes "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distribution

information by means of a computer system or network.” (UN, Crimes Related to Computer Networks: background Paper for the Workshop on Crimes Related to the Computer network, Tenth UN Congress on the Prevention of crime and the treatment of Offenders (Vienna, 10-17 April 2000): 5, paragraph 14).

The UN General Assembly has endorsed several resolutions dealing with its desire to witness progress regarding this issue. According to information provided by SchjØberg and Hubbard (S. Schjoberg, S. and A. M. Hubbard, Harmonizing National Legal Approaches in Cybercrime, International Telecommunication Union, WSIS Thematis Meeting on Cybersecurity (Geneva, 28 June-1 July 2005)), checking Resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, noted was the value of the Group of Eight principles, and states were urged to consider these principles; checking Resolutions 53/70 (1998), 54/79 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002), 58/32 (2003), and 58/199 (2003), all calling on member states “to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats.” (See UN Web site) These resolutions have the same motive to improve the cybersecurity awareness on both international and national levels.

In the Resolution 55/63, the General Assembly noted the value of the following measures to combat computer misuse:

(a) To ensure to eliminate safe havens for cybercriminals;

(b) To coordinate cooperation in the investigation and prosecution of cybercrime;

(c) To exchange information in fighting cybercrime;

(d) To train and equip law enforcement personnel to address cybercrime;

(e) To protect the security of data and computer systems from cybercrime;

(f) To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) To ensure mutual assistance regimes for the timely investigation of cybercrime and the timely gathering and exchange of evidence;

(h) To remind the general public of the requirement to prevent and combat cybercrime;

(i) To design information technologies to help to prevent and detect cybercrime;

(j) To take into account both the protection of individual freedoms and privacy

and the preservation of the capacity of Governments to fight cybercrime.

The General Assembly invites States “to take into account the above-mentioned measures in their efforts to combat the criminal misuse of information technologies,” and decided to maintain the question of the criminal misuse of information technologies on the agenda of its future session.

In the Resolution 56/121, the General Assembly invited States,

“When developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations.”

The resolution emphasized the value of the measures set forth in Resolution 55/63, and again invites States to take them into account in their efforts to combat the criminal misuse of information technologies. However, the General Assembly decided “to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice.”

It is necessary to mention that, besides the advantages, the disadvantages of the UN’s actions are also remarkable. The UN is a multifunctional international organization, which in some sense has malfunctioned over years. Focused on the current topic, it can be said that the consensus on cybercrime in this forum remains preliminary. The diversified legal systems of members of this gigantic organization hinder the conclusion of a fruitful agreement.

The focuses of international harmonization

From the above presentation on international actions in anti-cybercrime areas, we can further summarize the major common themes of these international organizations. These aspects mainly include promotion of security awareness on both international and national levels, harmonization of legislations, coordination and cooperation in law enforcement, and direct anti-cybercrime actions.

(i) Promotion of security awareness on international level

The representative actions in this aspect have been taken by the UN. The UN’s two Resolutions (55/63 (2000) and 56/121 (2001)) on Combating the Criminal Misuse of Information Technology reminded the importance of the Group of Eight

principles, and urged states to take these principles into account. Some other resolutions also called on Member States to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as promising measures to limit the threats. Other international organizations also made efforts to promote the security awareness on the international level. For example, after the 9/11 incidences, the APEC Leaders called for reinforcing APEC activities to protect critical infrastructure.

(ii) Promotion of security awareness on state level

All of the international organizations made efforts to promote security awareness at domestic level. For example, APEC guided its member states and regions to promote cybersecurity and tackle the threats by cybercrime. APEC also conducted a project for the developed states to support other states in training personnel. The Shanghai Declaration of 2002 also supported measures to fight against misuse of information.

(iii) Harmonization of legislation

Legal harmonization has been a major emphasis of work of various international organizations. Harmonization in the Europe started in 1980s and the recent achievement was Convention on Cybercrime. Other international organizations also endeavoured to legal harmonization. Early in 1981, the Interpol surveyed criminal laws of member states to explore defects in existing legislation, and made efforts to harmonize the laws. Today, the Interpol’s African Working Party on Information Technology Crime projects to propel the African states to sign and ratify the Convention on Cybercrime. The APEC also took steps to survey the laws and encouraged economies to enact comprehensive laws consistent with Convention on Cybercrime and the pertinent UN resolution. The EU Framework Decision of 2002 specifically granted the responsibility for the member states to criminalize offences of illegal access to and illegal interference with information systems. The REMJA urged states to criminalize cybercrime and harmonize laws, and consider the possibility to join the Convention on Cybercrime. The Commonwealth Model Law on Computer and Computer Related Crime expanded the criminal liability of the Convention on Cybercrime to include reckless liability. Through this Model Law, Commonwealth made efforts to criminalize cybercrime in the member countries. The Group of Eight Paris Conference discussed the public and private interact with the objective of implementing an international penal code for fighting cybercriminality.

The Okinawa Charter on Global Information Society further consented international collaboration and harmonization concerning cybercrime. International legislation harmonization is an imperative mission and convinced concern of the international organizations.

(iv) Coordination and cooperation of law enforcement

The Interpol's European Working Party on Information Technology Crime compiled the Computer Crime manual to provide a technical guidance in law enforcement. The Convention on Cybercrime also covers cooperative mechanisms in law enforcement against cybercrime. The EU discussed about retention of traffic data in 2001. The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA)'s Group of Experts on Cybercrime have been devoted to discover cooperation ways in the Inter-American system to combat cybercrime. The Group of Eight reviewed existing cooperation mechanisms and gaps, and made attempt to discover ways to fill these gaps. The group urged the states to increase criminalization, prosecution, investigation, and international cooperation. Denver Summit proposed to promote governments' technical as well as legal abilities to act in response to trans-territorial computer crimes. Birmingham Summit called for agreement on legal framework for evidence preservation and privacy protection, and agreements on international share of evidence to struggle against a broad scope of crimes, including cybercrime.

(v) Direct anti-cybercrime actions

The direct international anti-cybercrime actions include two fundamental aspects: cybercrime prevention and cybercrime investigation. They have been more valuable before the international harmonization in legislation can be acquired. Different organizations took individual actions with specific emphases. For example, the Interpol directly cooperated with credit card companies to fight against payment fraud. The OECD's Guidelines for Consumer Protection in the Context of Electronic Commerce 1999 emphasized the protection of consumers in e-commerce as that in traditional commerce. Guidelines for the Security of Information Systems and Networks 2002 called on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks".

From conversation to the European Convention

As one of the most outstanding achievements, international actions bred a comparatively effective implementation: the Convention on Cybercrime and its Protocol. The general purpose of the Convention is presented in the Preamble:

“Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation.” The purpose of the Protocol is to supplement the provisions of the Convention on cybercrime about the criminalization of acts of a racist and xenophobia nature committed through information systems (Protocol, Article 1).

The Convention has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both the domestic and international level of countermeasures, to achieve higher effectiveness in fighting against cybercrimes (Convention on Cybercrime, Preamble, Paragraph 9).

Articles 2-12 of the Convention required nations to criminalize the activities of illegal access to data and computer systems; illegal interception; data and systems interference; misuse of devices that can be used to enact the aforementioned crimes; computer-related forgery and fraud; content-related offences including child pornography; copyright crimes; and attempt, aiding or abetting. Article 13 of the Convention also establishes corporate liability, and sanctions and measures for these offences. Articles 3-7 of the Protocol requires nations to criminalize the activities of dissemination of racist and xenophobic information through information systems; racist and xenophobic motivated threat, racist and xenophobic insult; denial, gross criminalistic approval or justification of genocide or crimes against humanity, and the behaviours of aiding and abetting.

The Convention provides two constituent elements for cybercrimes. First, the Convention establishes criminal liability on the subjective element of intent. Sometimes, the constitution of some offences requires elements such as intent to

procure “economic benefit” in computer-related fraud provided by Article 8. Second, the Convention establishes criminal liability on the objective element of act “without right” in all offence provision (Convention on Cybercrime, Articles 2-12). The problems of what is an act committed intentionally, what is an act with right and without right, are all left to national law interpretation.

The Convention allows domestic laws provide additional constituent elements, and provides the possibility of a reservation (Ibid, Articles 40 and 42). Apparently, the Convention fully respects the decision-making of member states on the problem of criminal policy. As a result, we have the good reason to worry that the diversified implementation will decrease the consensus on the harmfulness of conducts and increase the possible obstacles in international actions. The negative effect of this kind of provision is expected to diminish the effectiveness of prolonged expensive international negotiation for the agreement, although the provision itself is exactly one of the contents negotiated and agreed.

The Convention has also been criticized by civil liberties groups concerned that it undermines individual privacy rights and expands surveillance powers too far, and is fundamentally imbalanced. As Taylor (2004) pointed out that, the Convention contains comprehensive, far-reaching powers of surveillance, search, and seizure, while lack of criterion of privacy protection and power limitation (G. Taylor, The Council of Europe Cybercrime Convention: A Civil Liberties Perspective (23 July 2004). Retrieved 14 January 2009, from http://crime-research.org/library/CoE_Cybercrime.htm). The basic concerns in the field of human rights are over-expansion of states’ power of surveillance, and over-criminalization of citizens’ behaviours: before information systems have been completely developed, the states would strictly take this borderless system under control; those who use information systems would voluntarily enter the tight legal encirclement. For those who use information systems before these legal instruments, they are to accept externally imposed constraints; while for those who use information systems after these provisions, they are born into the inherent limit. Both of these two groups of users may feel the loss of information freedom.

Despite the anxiety mentioned above, the Convention has unquestionably some influence on the worldwide consensus in relation to the predicament of cybercrime. We are capable of prospect that the Convention will become one of the important steps towards a broader international accomplishment.

Firstly, some countries take practical actions in ratifying the Convention. Total number of ratifications and accessions is 19 countries, including one non-member state of Council of Europe, the U. S., with 24 countries (including three non-member states of the European Council, Canada, Japan and South Africa) having signed the Convention, not followed by ratifications (See Council of Europe, Convention of Cybercrime, CETS No. 185, Chart of Signatures and Ratifications, (19 February 2007)). The treaty has entered into force only in a small number of countries, representing a small proportion in terms of land area and population. However, it is still an important step towards a broader consensus: "A little is better than none."

Secondly, besides successful endeavours, countries, including most signatory countries, are still on their way to ratifying the treaty. The Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response" in 2005 "strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international co-operation." (Council of Europe, Conclusions of the Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response" (Madrid, 12-13 December 2005)) The treaty has come into force in some of the Nordic countries, including Denmark, Iceland, and Norway, but Finland and Sweden are still seeking ratification though they are both countries of signature on the date opening for signature in 2001 (See for example, the Governmental Proposal HE 153/2006 of Finland aims at bringing the Convention on Cybercrime and the European Union's Framework Decision on Attacks against Information System into force in Finland and making relevant revision in domestic provisions according to the Convention (HE 153/2006, 3. Objectives and Central Proposals)).

However, this process proved hard without expectable number of countries took actions in the five-year period after the Convention was open to signatures. The pressure of not to ratifying the treaty from inside the countries seems a greater obstacle than differences in drafting the document. A significant obstacle comes from the difference of legislative styles between the Convention and the individual countries. Although many of the valid provisions in the current Finnish law do not need revision (HE 153/2006, Detailed Justifications), and whether the original Finnish Penal Code (which includes quite a few revisions concerning offences relating to data processing) is capable of dealing with all of the offences provided by the Convention or not is not tested in judicial practice, in order to cope with the Convention, the

Finnish legislature will have to add some new provisions to the Penal Code, including those concerning the offence of interference with and gross interference with the information processing systems, the offence of possession of instruments for cybercrime (covering the computer viruses), liability for inchoate cybercrime, and corporate liability, and so forth (HE 153/2006, General Justifications, 3. Objectives and Central Proposals).

A critical challenge of the Convention on Cybercrime to the conventional international legal cooperation lies in its absent demand for double criminality criterion. Decline of the criterion being a tendency, individual countries are far from implementing in domestic law. In accepting the Convention, individual countries shall have to revise domestic laws in the relevant area (Ibid.).

Thirdly, some other countries seek to model the Convention to provide prohibition for the types of conducts and to create procedural and international mechanisms in serving successful investigation and prosecution. Flexibilities of the Convention may have a positive effect in leaving member states the alternative to using different methods and languages in their domestic law. This may lead the Convention to a wider application to covering more and diversified legal systems. South Africa has implemented substantial criminal provisions in consistence with the Convention. The U. S. asserted that its domestic law does not require to be revised. Japan is considering filling the gap between its domestic law and the Convention. At least, among APEC economies, Taiwan, the Philippines, and Hong Kong consider taking the Convention as the basis on which they carry out the legislative amendment.

Fourthly, some international organizations are propelling cooperation in promoting the member states' access to Convention. As mentioned above, in the framework of Interpol, the African Working Party on Information Technology Crimes works for propelling domestic legislation and joining the Convention. To some extent, this will facilitate the African countries to acknowledge the legislation consistence and harmonization. The APEC, the EU, and the REMJA V of the OAS also took actions to spread the Convention in its member states.

Fifthly, there are also efforts to develop cybercrime legislation beyond the Convention. As mentioned above, the Commonwealth's model law represents a breakthrough in extending the criminal liability in the aspect of mens rea of offences of interfering with data, interfering with computer systems, and illegal devices to

include reckless liability. Some Commonwealth's Member States are also on their way towards legislations modelling the Convention and the model law.

Finally, in fact, most countries, particularly some countries where cybercriminals are usually let at large have taken no action considering the importance of the Convention. Those countries have very specific interests in accommodating, what may be considered "criminal" in other countries but are "legal" in these countries, the web sites, services, or even sales of goods online. The potential cybercrime perpetrators, regardless of wherever their nationalities belong to, also seek asylum in those countries to escape punishment by other countries that are seeking extending their judicial arms to deal with cases committed inside their sovereign territory and committed by their citizens outside their territory.

Although the Convention on Cybercrime has been attracting increasing attention from both domestic and international levels, it is necessary to point out that, after the Convention formed a document, the enthusiasm and efforts of other international entities towards higher degree of international harmonization of legislation have been to some extent weakened. It is neither the purpose, nor the side effect of Convention. However, a ready instrument must have the negative influence on the otherwise unsettled disputes on the problems of cybercrime deterrence. Both the advantages and dizadvantages of the Convention will bring about more cautious discussion and better plan will be discouraged from being implemented. At least, the similar but different schedules for international treaties, in either broader or narrower scope, have seen an interruption with the pass of the Convention. The Convention thus becomes not only a mutual compromise of the member states, but also a turning point of the knowledge and experiences on cybercrime punishment and prevention.

Traditionally, new legal instruments have usually been the subject of academic annotation right after its implementation, while legislature is usually reluctant to change existing legal instruments. These two factors further determine the unfortunate fate of the better and newer proposals, particularly those proposals with more or less better factors that ever paralleled the implemented one. In a word, we can say that classics were good, but classics hinder better classics; consensus are good, but consensus always hinders better consensus: and the Convention is good, but it potentially hinders a better convention.

Although the Convention was also appraised by politicians, such as the U. S. President George W. Bush, as "providing for broad international cooperation in the

form of extradition and mutual legal assistance", and containing "safeguards that protect civil liberties and other legitimate interests" (Bush 2003), the effectiveness of Convention's cooperative framework is subject to reasonable doubt without a majority of countries' access to the agreement (Goldsmith 2005). Authors such as Archick proposed that the Convention's arm would not be long enough to reach the countries that are regarded as "haven" for cybercriminals (Archick 2004): attacks are launched from those countries, but the countries do not join the agreement. Consequently, the countries with law and without law, or being the member and being non-member of the Convention, have to encounter mutual conflicts. The situation confronting the international society is obviously still the tardiness of the acceptance of the existing instruments and the lack of a universal agreement.

The limited progress in the international harmonization

International level of consensus on criminal law has not been achieved. Previously, the criminalization of war crime, crime against peace, crime against humanity, genocide, torture, and other crimes have been the successful examples. The application of pertinent agreements in specific courts demonstrated that international forum can acquire certain achievements prior to legislation on the national level. The traditional international criminal law aimed at harmonising substantive law and coordinating procedural law on offences that have existed in society ever since the coming into being of humankinds (The origination of human beings has been an unsolved theoretical problem. Genesis theory and evolutionary theory might be the most influential arguments). Presently, what the countries are eager to schedule was an international agreement on offences with a history of several decades. The anxiousness for success, the absence of trial practice, the lack of accumulation of experience and knowledge, the alienation between legislature and general public, and the different interests between countries, all deliver the international consensus to the least limit. It is inevitable that during the draft stage and particularly after the Convention on Cybercrime was opened for signature, many commentators published their evaluation and criticism (For an overall evaluation on the Convention on Cybercrime, see Jones 2005). The Convention was also subject to criticisms from individuals and organizations, such as American Civil Liberties Union and others).

Combined with other progress made in the international harmonization, the most important unsolved problem may be the limited participants and limited consensus.

Firstly, the international harmonization hitherto has been primarily the forum of developed countries. The working mechanism of an effective international treaty is for all of the signatory countries to take effective action and preserve a common theatre. The treaty is not aimed at any third party and thus the third party is not restrained by it. The participating countries of the Convention on Cybercrime are limited, only representing a limited population. Along with the development of Internet globally, the number of cybercrimes will be correlated with the population base of Internet penetration, and the global population base. Most of the present international harmonization actions have not incorporated the countries with the largest population. This will make the actions less effective. Considering the characteristics of cybercrime, the "safe haven for criminals" can only be eliminated when almost all of the sovereign states have access to one agreement and almost all of the online users are subject to the power of law enforcement. Although an international document can be modelled by member states in making domestic laws, the expectation should not be too high towards a timely update in a similar pace.

Secondly, another limitation is that a lower level of consensus has been reached. Unlike traditional offences in the international criminal law, which have rarely been penalized in domestic law, cybercrime was firstly implemented in legislation of national level. In many countries, domestic legislation on offences such as genocide, crime against peace and others did not happen before the countries were subject to the obligation of international treaties. The situation of cybercrime is that countries that have already enacted laws assisted or forced the countries that have not enacted laws to enter a consensus. As a whole, the international cooperation on preventing cybercrime is more sluggish than domestic legislation; its impact on domestic legislation is, nonetheless, undeniable. Domestic laws should be amended according to international instruments so that the measures provided in the international instruments can be effectively carried out. An agreement in a wider scope of issues in cybercrime is also necessary in ensuring effective law enforcement. However, such an agreement is still lacking. The efforts of various international organizations should be integrated into a more unified action.

Thirdly, there is a tendency of pluralization of the international harmonization. In regulating or deregulating the information community, different interest groups

stay on different standpoints. In criminalizing and decriminalising the online activities, different players hold different opinions. Different organizations proposed countermeasures for the benefit of a certain number of their member states. Yet other organizations opposed any kinds of plans for imposing constraints on free use of information systems. The mechanism is that while one interest group is anxious about the misuse of information systems, another group may concentrate on the side effect of anti-misuse actions. Various international harmonization actions are full of trade-off of interests and contrast of powers. The marathon process of negotiation inherited the inherent style of international actions.

Fourthly, another tendency is the regularization of the international harmonization. The effect of the international harmonization is less significant compared with the efforts. The role of the UN as a universal international organization seems limited in arrange an international treaty in this area. If the United Nation's frequent "call" does not motivate member states to legislate on cybercrime, a universal agreement should be a better alternative in promoting consensus. The UN may have the opportunity to incorporate consensus reached in different fields into the above-mentioned unified action.

Conclusion

Globalization does not mean globalized welfare at all. Globalized information systems accommodate increasing number of trans-national offences. The network context of cybercrime makes it one of the most globalized offences against the present and the most modernized threats against the future. We can take actions in two different ways to solve this problem. One is to divide information systems into segments bordered by state boundaries. The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Roman, Greece, and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems will not be an imaginable practice. Information systems become the unique empire without tangible territory and an emperor in the 21st century.

Offences happening in information systems are not possible to receive

punishment from this system. Rather, they are punishable by territory-based states that they cross. It is increasingly stringent and necessary to establish an international cooperation system on punishing cybercrime. Various international organizations have taken actions to solve the problem in different forums and on different levels.

Convention on Cybercrime is acknowledged as a landmark in the sphere of international harmonization of cybercrime law (See Council of Europe Cybercrime Conference, High-level Conference on the Challenge of Cybercrime, (15-17 September, 2004): Conclusions). However, besides that it represents a significant step forward, in order to serve as a deterrent, more states will have to sign the Convention and abide by its mandates. The international harmonization centred by the Convention is obviously limited and necessary to extended to more participating member states and even wider scope of issues. The final effect should be achieved only through a universal agreement on combating cybercrime. The UN may have higher potential to implement such universal measures. However, we should not expect an instantaneous reaction from any of the international organizations, because not so much attention and interests of these international organizations are concentrated on the problem of crime or precisely, cybercrime. While they are devoted to deal with more important international affairs, the threats against critical information infrastructure are becoming more serious, until they are listed in the top list of these organizations' schedule. Consequently, the international level of consciousness and international level of call for national level of consciousness still necessitates effective actions, to keep under reassess and renew as necessary the present international legal frameworks, offer a forum for broader international conversation with an outlook to increasing and advancing international law enforcement cooperation among national authorities, consider the influences of the novel and emerging issues on international law enforcement cooperation, make recommendations on capacity-building, and give equal concern about the situation in countries of different stages of development to avoid a futureless future of information chaos.

References

APEC. 2003. Conference Report: Cybercrime Legislation and Enforcement Capacity Building Project, 21-25 July, Bangkok, Thailand.

Archick, K. 2004. Cybercrime: The Council of Europe Convention, CRS Report for Congress. Order Code RS21208, Congress Research Service, 22 July.
Bourne, R. 2002. Commonwealth Law Ministers' Meeting: Policy Brief. Lodon: Commonwealth Policy Studies Unit.
Bush, G.W. 2003. Message to the Senate of the United States on the CyberCrime Convention, Office of the Press Secretary, 17 November.
Commission of the European Communities 2002. Proposal for a Council Framework Decision on Attacks against Information System, COM (2002) 173 final, 2002.
E-Security Task Group 2003. E-Security Task Group, Cybercrime Legislation and Enforcement Capacity Building Project, 21-25 July, Bangkok, Thailand.
European Union Forum on Cybercrime (EUFC) 2001. Discussion Paper for Expert's Meeting on Retention of Traffic Data, Brussels.
Fooner, M. 1989. Interpol: Issues in World Crime and International Criminal Justice. New York and London: Plenum Press.
Goldsmith, J. 2005. The Internet and the Legitimacy of Remote Cross-Border Searches, Chicago Public Law and Legal Theory Working Paper, Number 16, The Law School, The University of Chicago.
Grabosky, P.N. 2004. Global Dimension of Cybercrime, Global Crime, Volume 6, Number 1, pp. 146-157.
Jones, C.W. 2005. Council of Europe Convention on Cybercrime: Themes and Critiques. Workshop on the International Dimensions of Cyber Security, hosted by the Georgia Institute of Technology and Carnegie Mellon University, 6-7 April.
McConnell International 2000. Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information. December. Retrieved 14 January 2009, from http://www.witsa.org/papers/McConnell-cybercrime.pdf
Organization for Economic Cooperation and Development. 2002. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.
Pihlajamäki, Antti. 2004. Tietojenkasittelyrauhan rikosoikeudellinen suoja: datarikoksia koskeva saantely Suomen rikoslaissa (The Protection of Data Processing under Criminal Law: Provisions on Data Crimes in the Finnish Criminal Code), Helsinki: Suomalainen lakimiesyhdistys.
Police Commissioners' Conference Electronic Crime Working Party. 2000. The Virtual Horizon: Meeting the Law Enforcement Challenges: Developing an

Australasian Law Enforcement Strategy for Dealing With Electronic Crime. Scoping Paper, Adelaide: Australasian Centre for Policing Research, Report Series No: 134.1.
Putnam, T.L., and Elliott, D.D. 2001. Chapter 2- International Responses to Cyber Crime. In: Abraham D. Sofaer, and Seymour E. Goodman, (Eds.), The Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution, pp. 35-68.
Schjølberg, S., and Hubbard, A.M. 2005. Harmonizing National Legal Approaches in Cybercrime, 10 June, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June-1 July.
Schjølberg, S., and Tingrett, M. 2004. Computer-Related Offences- A Presentation at the Octopus Interface 2002. Conference on the Challenge of Cybercrime, 15-17 September, Council of Europe, Strasbourg, France. Retrieved 14 January 2009, from http://cybercrimelaw.net/documents/Strasbourg.pdf
Sieber, U. 1996. Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society. Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16 July.
Sieber, U. 1998. Legal Aspects of Computer-Related Crime in information Society, The COMCRIME-Study for the European Commission, 1 January.
Sofaer, A. D., et al. 2000. A Proposal for an International Convention on Cyber Crime and Terrorism, Centre for International Security and Cooperation.
Sofaer, A. D., and Goodman, S. E. 2005. The Transnational Dimension of Cyber Crime and Terrorism, Hoover Press.
United Nations Crime and Justice Information Network (UNCJIN). 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime. International Review of Criminal Policy, Numbers 43 and 44.
Wasik, M. 1991. Crime and the Computer. Oxford: Clarendon Press.
National Computer Emergency Response technical Team/Coordination Centre of China (CNCERT/CC), APEC Telecommunications and Information Working Group Guide on Policy and Technical Approaches against Botnet, December 2008.